SÄHKÖPOSTIJÄRJESTELMÄN TOIPUMISSUUNNITELMA ELISA APPELSIINI OY:N ASIAKKAALLE

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Visamäki, Tietojenkäsittelyn koulutusohjelma

kevät, 2017

Tuomo Andelin

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutusohjelma
Visamäki

Tekijä Tuomo Andelin **Vuosi** 2017

Työn nimi SÄHKÖPOSTIJÄRJESTELMÄN TOIPUMISSUUNNITELMA ELISA APPELSIINI OY:N ASIAKKAALLE

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli toteuttaa sähköpostiympäristön toipumissuunnitelma Elisa Appelsiinin asiakkaalle projektina. Tarkoituksena oli perehtyä toipumissuunnitelmaan projektina sekä Microsoftin Exchange Server 2013 -sähköpostipalvelinsovellukseen.

Toipumissuunnitelmaan kuvattiin asiakkaan nykyinen sähköpostiympäristö konfiguraatioineen ja riippuvuuksineen. Ympäristön kuvauksen lisäksi toipumissuunnitelmaan dokumentoitiin mahdolliset ongelmatilanteet ja niiden toipumissuunnitelmat.

Opinnäytetyössä kuvataan aluksi toipumissuunnitelman perusteet. Toipumissuunnitelman jälkeen tutustutaan Exchange Server 2013 -ohjelmistoon, jonka päälle asiakkaan sähköpostiympäristö on asennettu.

Toipumissuunnitelma käydään opinnäytetyössä läpi raportin muodossa ja asiakkaalle palautettu toipumissuunnitelma on liitteenä.

Opinnäytetyössä selvisi, miten yhden palvelimen ympäristön ylläpito on helpompaa kuin usean palvelimen muodostama korkean saatavuuden toteutus. Toisaalta toipumissuunnitelmassa kuvatut vikatilanteet aiheuttavat aina palvelussa tuotantokatkon yhden palvelimen ympäristössä, kun taas korkean saatavuuden ratkaisussa ei välttämättä katkoa havaita.

Toipumissuunnitelmaprojektin aikana selvisi, että dokumentin tärkein osa on ongelmatilanteiden toipumismenetelmät.

Avainsanat **Toipumissuunnitelma, Exchange, saatavuus, vikasietoisuus**

Sivut 46 sivua, joista liitteitä 16 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology
Visamäki

Author Tuomo Andelin **Year** 2017

Subject Disaster Recovery Plan for an email environment, Case Elisa Appelsiini's Customer

ABSTRACT

The purpose of this thesis was to provide my employer's customer with a disaster recovery plan for their email environment. The disaster recovery plan also includes a description of the customer's current email environment including configuration and dependencies. The Disaster recovery plan also includes possible disaster recovery scenarios and the steps to rectify them.

The thesis includes an overview of disaster recovery plan basics and then a general glance of Exchange Server 2013 software environment which is the software platform for the customer's email system.

The actual disaster recovery plan is included as an appendix and and it is discussed in the report of the thesis.

During this thesis, it discovered how easy it is to maintain and manage a single server email environment as opposed to a multiple-server environment. On the other hand, the disaster scenarios described in the disaster recovery plan will always result in an outage in a single server environment, but not necessarily in a high availability configuration such as multiple server environment.

Keywords Disaster Recovery Plan, Exchange, Availability, Redundancy

Pages 46 pages including appendices 16 pages

KÄSITTEET

MCSE	Microsoft Certified Solutions Expert on Microsoftin sertifiointi asiantuntijoille, jotka rakentavat IT-ympäristöjä käyttäen hyväksi ko. teknologiaa.
RPC Over http	Remote Procedure Call Over Hypertext Transfer Protocol on Microsoftin käyttämä teknologia, jolla sähköpostiasiakkaat voidaan yhdistää internetin kautta sähköpostijärjestelmään turvallisesti ja tehokkaasti.
ActiveSync	Microsoftin kehittämä sovellus jolla mobiililaitteet voivat synkronoida dataa.
POP	Post Office Protocol on yksinkertainen sähköpostin hakemiseen tarkoitettu protokolla.
IMAP	Internet Message Access Protocol on sähköpostien lukemiseen tarkoitettu protokolla.
UM	Unified Messaging -teknologioilla voidaan yhdistää ääni- ja sähköpostipalveluita. Esimerkiksi puhelinvastaaja joka siirtää saapuneen puheviestin äänitiedostona sähköpostilaatikkoon.
DMZ	Aliverkko, joka yleensä yhdistää sisäverkon ja internetin.
Snapshot	Termi jota käytetään tietystä ajankohdasta otetusta varmistuksesta.
DNS	Domain Name System muuttaa verkkonimet IP-osoitteiksi.
DHCP	Dynamic Host Control Protocol jakaa IP-osoitteet laitteille verkossa.
Private Key	Salausavain, jota käytetään datan salaamiseen ja salauksen purkamiseen.
Certification Authority	CA jakaa sertifikaatteja. Sisäverkossa CA on palvelin ja internetissä sertifikaattien jakeluun erikoistunut yritys.

RAID	Redundant Array of Independent Disks on teknologia jolla kovalevyjä voidaan yhdistää muodostamaan vikasietoisia kokonaisuuksia.
JBOD	Just a Bunch of Disks viittaa kovalevykokoelmaan.
SMPT	Protokolla joka välittää viestejä sähköpostipalvelimien välillä.
AD Schema	Määrittelee kaikki objektit ja attribuutit joita Active Directory käyttää datan tallennukseen.
URL	Uniform Resource Locator on internetosoite.
TLS salaus	Transport Layer Security on salausprotokolla jota käytetään esimerkiksi SMTP-, POP-, ja IMAP-yhteyksien salaamiseen.

SISÄLLYS

1 JOHDANTO 1

1.1 Aiheen rajaus, työn tavoitteet ja kysymyksen asettelu 1

2 TOIPUMISSUUNNITELMAN PERUSTEET 3

2.1 Toipumissuunnitelmista vastaavat henkilöt 3
2.2 Toipumistilanteen johtaminen ja organisointi 4
2.3 Toipumissuunnitelman käynnistämisen syyt 4
2.4 Toiminta häiriön aikana 5
2.5 Toipumissuunnitelmien dokumenttien sijainti, ylläpito ja koulutus 5
2.6 Toipumissuunnitelma Exchange Server 2013 -ympäristölle 5

3 EXCHANGE SERVER 2013 7

3.1 Exchange 2013 -palvelinroolit 7
3.2 Roolien vikasietoisuus 8
3.3 Riippuvuudet 9
3.4 Suositeltu arkkitehtuuri 10

4 TOIPUMISSUUNNITELMA 19

4.1 Versionhallinta 19
4.2 Yhteystiedot ja yhteistyökumppanit 20
4.3 Palvelutaso 20
4.4 Ympäristön kuvaus 21
4.5 Konfiguraatio 21
4.6 Transport-asetukset 22
4.7 Tekniset riippuvuudet 24
4.8 Ennakoidut vikatilanteet 25

5 YHTEENVETO 28

6 LÄHDELUETTELO 29

Liitteet

Liite 1 Toipumissuunnitelma

1 JOHDANTO

Työnantajani Elisa Appelsiini Oy:n asiakas on tilannut toipumissuunnitelmaprojektin IT-infrastruktuurilleen. Toipumissuunnitelma jaetaan alaosiin teknologioittain, ja siihen kuuluvat muun muassa sähköpostijärjestelmän, tietokantojen, Active Directoryn, Citrixin ja VMWaren toipumissuunnitelmat. Projektia edistää virtuaalinen projektitiimi Appelsiinilla, johon kuuluu projektipäällikön lisäksi vaihteleva määrä eri teknologioiden asiantuntijoita spesialisteista ylläpitäjiin, arkkitehteihin ja konsultteihin. Minulle tarjoutui mahdollisuus laatia sähköpostijärjestelmän toipumissuunnitelma ja toteuttaa siitä samalla opinnäytetyö kehitysprojektina.

Minulla on työkokemusta IT-järjestelmien ylläpitotehtävistä noin 10 vuoden ajalta, joista viimeisen kahden vuoden aikana olen profiloitunut ylläpitämään erityisesti asiakkaidemme Microsoft Exchange Server -sähköpostiympäristöjä. Samalla minulle on kehittynyt kiinnostus tätä teknologiaa kohtaan, ja tavoitteenani on sertifioitua MCSE-asiantuntijaksi.

Opinnäytetyön toimeksiantajana toimii pörssiyhtiö Elisan IT Business Unit Elisa Appelsiini Oy, joka tarjoaa yritysasiakkailleen IT-palveluita ylläpidosta sovelluskehitykseen.

1.1 **Aiheen rajaus, työn tavoitteet ja kysymyksen asettelu**

Projektissa laaditaan toipumissuunnitelmat asiakkaalle ja asiakkaan tavoitteet toipumissuunnitelmalle ovat seuraavat:

1. sähköpostia voidaan lähettää ja vastaanottaa organisaation sisä- ja ulkopuolelta
2. sähköpostilaatikoiden sisältö on ajan tasalla
3. postinkulkuun liittyvät asetukset, kuten jakelulistat, ovat ajan tasalla, palvelukatkokset ja datan menetys minimoiden.

Käytännössä toipumissuunnitelmaan kuvataan tämänhetkinen sähköpostiympäristö, sen riippuvuudet muihin järjestelmiin, yleisimmät ongelmatilanteet (Disaster) ja niille toipumissuunnitelma (Disaster Recovery Plan). Olemme sopineet, että suunnitelma kirjoitetaan kohderyhmälle, joka koostuu teknisistä asiantuntijoista. He voivat suunnitelmaa hyväksikäyttäen suorittaa tarvittavat toimenpiteet, jotta asiakkaan asettamat tavoitteet toteutuvat.

Toipumissuunnitelman lisäksi avaan opinnäytetyössä myös Microsoftin referenssi-arkkitehtuuria, jossa kuvataan optimoitu ratkaisu kyseessä olevalle teknologialle ja niin kutsutut parhaat käytännöt (Best Practices) käytössä olevalle järjestelmälle.

Opinnäytetyö vastaa seuraaviin kysymyksiin:

Mitä asioita toipumissuunnitelmaan kuuluu?

Kuinka erilaisista ja yleisimmistä katastrofitilanteista toivutaan ajan ja datan menetys minimoiden?

Millainen sähköposti-infrastruktuurin pitäisi olla, ettei loppukäyttäjälle tulisi palvelukatkoja?

Elisa Appelsiinin asiakas on halunnut pysyä nimettömänä, mutta kyseessä on noin kahdensadan sähköpostikäyttäjän ympäristö. Suomessa mittakaavassa yritys on keskikokoinen, mutta kansainvälisesti ja IT-arkkitehtuuri huomioiden yritys on pieni. Yrityksen koko asettaa erityiset haasteet, kun kapasiteetti referenssi-arkkitehtuurin toteuttamiseen ei välttämättä ole riittävä, vaan joudutaan operoimaan sähköpostipalvelua yhdellä palvelimella ja perinteisillä datan varmistuskeinoilla. Tämä johtaa ongelmatilanteissa aina palvelukatkoon. Opinnäytetyön toipumissuunnitelmaosioissa asiakkaan nimi korvataan sanalla asiakas.

2 TOIPUMISSUUNNITELMAN PERUSTEET

Termi toipumissuunnitelma tulee englanninkielisistä sanoista Disaster Recovery Plan. Toipumissuunnitelma on dokumentaatio, jossa kuvataan prosessit, joilla saadaan jokin IT-arkkitehtuurin palvelu palautettua ongelmatilanteesta, kun tavalliset ylläpidolliset toimenpiteet eivät siihen riitä.

Dokumentaatioon kuvataan suunnitelman kohteena olevan palvelun arkkitehtuuri ja mahdolliset ongelmatapaukset sekä prosessit, joilla niistä toivutaan.

Arkkitehtuurin kuvaus sisältää kaikki tiedot palvelun konfiguraatiosta, jotta palvelu voidaan uudelleen asentaa dokumentaatiota hyväksikäyttäen. Toipumissuunnitelman kohderyhmänä ovat tavanomaisesti järjestelmäasiantuntijat ja muut IT-alan työntekijät, jotka ovat vastuussa kyseessä olevan teknologian toimivuudesta.

Palvelut, joille toipumissuunnitelmia kirjoitetaan, voivat sisältää sekä fyysisten komponenttien että sovellusten ongelmatilanteita. Toipumissuunnitelmaan pyritään kuvaamaan mahdollisimman paljon erilaisia ongelmatilanteita, joihin suunnitelman avulla voidaan löytää ratkaisu ja palauttaa palvelu toimintaan.

Projektissa on ennalta sovittu, että kaikkiin järjestelmäkohtaisiin toipumissuunnitelmiin kuvataan seuraavat asiat:

- järjestelmän toteutusdokumentaatio
- järjestelmäkohtaiset ongelman rajoittamistoimet
- järjestelmäkohtaiset toipumismenetelmät ja niiden käytön seuraukset
- tuotantokelpoisuuden testaaminen
- järjestelmän käynnistäminen ja toimivuuden testaaminen käynnistyksen jälkeen
- järjestelmän tuotantokäytön aloittaminen

Dokumentaation ylätasolla, ennen järjestelmäkohtaisia toipumissuunnitelmia, käydään läpi toipumissuunnitelmista vastaavat henkilöt, toipumissuunnitelman johtaminen ja organisointi, toipumissuunnitelman käynnistämisen syyt, toiminta häiriön aikana sekä dokumentaation sijainti, ylläpito ja koulutus. (Elisa Appelsiini 2016.)

2.1 **Toipumissuunnitelmista vastaavat henkilöt**

Toipumissuunnitelman toimeenpanosta vastaavat esimerkiksi seuraavat henkilöt:

Projektipäällikkö, joka vastaa muutoksista toipumissuunnitelmiin,

Manager On Duty, joka vastaa tiedottamisesta toimittajan puolelta,
Major Incident Manager, joka vastaa toipumissuunnitelman toteutumisesta ongelmatilanteessa,
MIM-prosessin omistaja, joka on asiakkaan IT-päällikkö.

2.2 Toipumistilanteen johtaminen ja organisointi

Laajassa häiriötilanteessa toimittaisiin kuvan 1 mukaisesti. Tilanteen havaitsee useimmiten asiakas tai valvontaa suorittava asiantuntija. Havainnoitsija tekee ensimmäisen arvion siitä, onko kyseessä laaja häiriö. Mikäli näin on, havaitsija ottaa yhteyttä Major Incident Manageriin joka tekee lopullisen päätöksen siitä, onko kyseessä laaja häiriötilanne.

Rooli	Tehtävät/Vastuut
Prosessin omistaja	Vastaa laajavaikutteisen häiriönhallintaprosessin kehittämisestä ja seurannasta
Major Incident Manager	Häiriönhallinnan sekä kaikkien siihen liittyvien toiminnan ohjaus Nimeää viankorjaukseen osallistuvat asiantuntijat ja tiedottajan Tekee kaikki palvelun palauttamiseen liittyvät päätökset Kerää palvelupoikkeamaraporttiin tarvittavat tiedot, tai nimeää kirjurin Kutsuu häiriönpoiston jälkeen koolle jälkiselvitysryhmän, joka tuottaa loppuraportin jatkotoimenpiteineen
Ulkoinen Tiedottaja	Tiedottaa häiriötilanteen etenemisestä asiakkaalle
Sisäinen Tiedottaja	Tiedottaa häiriötilanteen etenemisestä Major Incident Managerin määrittelemällä jakelulistalla
Asiantuntija(t)	Osallistuu viankorjaukseen Asiantuntijoiden tehtävänä on tuottaa kiertotie tai ratkaista vikatilanne pysyvästi Laajavaikutteisen häiriön hoitoon osallistuvat asiantuntijat vapautuvat muista tehtävistä väliaikaisesti Major Incident Managerin päätöksellä
Tiedotettavat	Tiedotettavat eivät osallistu viankorjaukseen Vastaanottavat tiedotteet ja ohjaavat tiedon eteenpäin tilanteen niin vaatiessa

Kuva 1. Toipumistilanteen organisointi. Henkilöt, jotka osallistuvat toipumistilanteeseen (Elisa Appelsiini 2016).

2.3 Toipumissuunnitelman käynnistämisen syyt

Termit laajavaikutteinen häiriö (Major Incident) ja laajavaikutteisen häiriön hallinta (Major Incident Management) tulevat ITIL-viitekehyksestä, ja näillä pyritään kuvaamaan mitä tahansa laajavaikutteista palvelupoikkeamaa. ITIL tulee sanoista Information Technology Service Management, joka on kokoelma parhaita käytäntöjä tietojärjestelmien palvelunhallintaan. ITILiä käytetään yleensä raamina konsepteille ja käytännöille joista organisaatiot johtavat omat parhaat käytännöt esimerkiksi tietojärjestelmien ylläpitoon. Palvelupoikkeama määritellään taloudellisen tai käyttäjämäärän laajuuden perusteella normaaliksi tai laajavaikutteiseksi häiriöksi.

2.4 Toiminta häiriön aikana

Häiriön aikaiseen toimintaan kuuluvat seuraavat toimenpiteet: Ongelmatilanteen tunnistaminen, henkilöiden resursointi ongelman ratkomiseen sekä tiedotus sovituille tahoille. Tiedottamisessa käytetään yleensä vakioitua formaattia, jossa on mainittu ongelman alkamisaika, palveluvaikutus sekä laajuus. Jos tiedossa on arvioitu korjausaika tai väliaikaisratkaisu, ne mainitaan myös tiedotteessa.

2.5 Toipumissuunnitelmien dokumenttien sijainti, ylläpito ja koulutus

Dokumentaation fyysinen versio sijaitsee asiakkaan tiloissa tietoturvallisessa kassakaapissa, sähköinen versio asiakkaan dokumenttien hallintajärjestelmässä ja Elisa Appelsiinin versio Wiki-järjestelmässä. (Elisa Appelsiini 2016.)

2.6 Toipumissuunnitelma Exchange Server 2013 -ympäristölle

Exchange Server 2013 -ympäristön sähköpostitietokantojen varmistukset ovat keskeisiä, kun toipumissuunnitelmaa hahmotellaan. Suunnitelmissa on otettava huomioon RPO (Recovery Point Objective) ja RTO (Recovery Time Objective), jotka määritellään yleensä toimittajan ja asiakkaan välisessä palvelusopimuksessa. RPO ja RTO ohjaavat omalta osaltaan palvelun tuottamista. (Elfassy 2014, 698.)

RPO on suurin hyväksyttävä aika menetetylle datalle eli kuinka pitkältä ajalta on hyväksyttävää menettää dataa ongelmatilanteen sattuessa. Esimerkki: Yrityksen sähköpostitietokannat kopioidaan varmistusnauhalle joka yö kello 01:00. Aamulla kello 08:00 tuotannon tietokanta korruptoituu niin, ettei se ole käytettävissä, eikä sitä saada enää kuntoon. Palautus varmistusnauhalta aloitetaan ja palautetaan tilanne, joka oli kello 01:00 yöllä. Tämän seurauksena dataa on menetetty seitsemän tunnin ajalta. Jos RPO on seitsemän tuntia tai suurempi, datan hävikki sopii ennalta määrättyihin raameihin. Jos RPO ylitetään, voidaan toimittajalta vaatia esimerkiksi kompensaatio menetetystä datasta. (Joffel 2011.)

RTO on aika, jonka sisällä palvelu pitää saada palautettua toimintaan, toisin sanoen, kuinka kauan palvelu voi olla alhaalla loppukäyttäjän näkökulmasta.

Usein RPO ja RTO ovat osa suurempaa palvelutasosopimusta (Service Level Agreement, SLA), jossa yleensä määritellään palveluiden vaatimustasot. Edellä mainittuja tietoja voidaan käyttää hyväksi, kun suunnitellaan sähköpostipalvelun varmistuksia.

Tietokantojen lisäksi tärkeä on myös Exchange Server 2013 -palvelin eli alusta, jolla sähköpostipalvelu pyörii. Exchange Server 2013 toimii vain Windows Server -käyttöjärjestelmässä. Mikäli palvelin vikaantuu, sitä ei voida palauttaa varmistuksista kuten useat muut palvelimet vaan se on asennettava uudelleen. Active Directory -hakemistopalvelulla, joka tallentaa kaikki tärkeät Exchange Server 2013 -konfiguraatiot, on erittäin tärkeä rooli mahdollisessa uudelleen asennuksessa.

3 EXCHANGE SERVER 2013

Exchange Server 2013 on Microsoftin ratkaisu yritysten sähköpostipalveluksi. Exchange Server 2013 tarjoaa asiakkaille sähköposti-, kalenteri- sekä yhteystietopalvelut eri päätelaitteille, kuten tietokoneille ja mobiililaitteille (Microsoft n.d.).

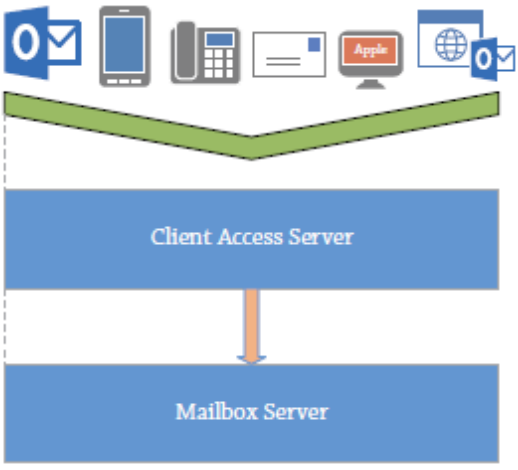
3.1 **Exchange 2013 -palvelinroolit**

Smith kuvaa blogiartikkelissaan kattavasti Exchange-palvelinrooleja. Exchange Server 2013 koostuu kahdesta Windows-palvelinroolista, Mailbox ja Client Access, jotka voidaan asentaa samalle palvelimelle tai eriyttää Client Access- ja Mailbox-palvelimiksi. Aikaisemmissa Exchange Server -versioissa, kuten Exchange Server 2010:ssä, oli useita palvelinrooleja. (Smith 2013.)

Exchange Server 2010 -arkkitehtuuri koostuu viidestä palvelinroolista:

1. **Edge Transport** hoitaa reitityksen Internetin ja Exchangen välillä sekä haittaohjelmien että roskapostin suodatuksen verkon reunalla.
2. **Hub Transport** keskittyy sisäiseen reititykseen ja käytäntöjen toimeenpanoon.
3. **Mailbox** säilyttää postilaatikoiden datan.
4. **Client Access** vastas asiakasyhteyksistä ja web-palveluista.
5. **Unified Messaging** on tarkoitettu puhepalveluille, kuten automaattiselle vastaajalle. (Smith 2013.)

Roolien sirpaloituminen aiheutti ylläpitäjille haasteita ja turhia rajoituksia, joita Exchange Server 2013:ssa pyrittiin poistamaan yksinkertaistamalla ja erityisesti vähentämällä rooleja (Kuva 2). Tämän vuoksi Exchange Server 2013 pitää sisällään vain kaksi roolia. (Smith 2013.)



Kuva 2. Exchange Server 2013 -palvelinroolit ja loppukäyttäjien laitteet *(*Elfassy 2014, 209)

Client Access Server -rooli välittää pääasiassa asiakasyhteyksiä sähköpostijärjestelmään. Palvelin autentikoi pyynnöt, paikallistaa postilaatikon ja välittää asiakasliikenteen oikealle Mailbox-palvelimelle ja Mailbox-palvelimilta internetiin. Tarkemmin sanottuna Client Access -palvelin tukee asiakasprotokollia, kuten Outlook Anywhereä (RPC Over HTTP), mobiililaitteille tarkoitettua ActiveSynciä ja POP-, IMAP- sekä SMTP-viestien välitystä internetistä ja internetiin, mukaan lukien UM puhelu -reititys.

Mailbox Server -rooli sisältää kaikki ne komponentit ja protokollat, jotka prosessoivat ja tallentavat dataa. Data tallennetaan tietokantoihin ja tietokannoista voidaan muodostaa tietokannan käytettävyysryhmiä. Tämän seurauksena tietokannan aktiivinen, käytössä oleva kopio sijaitsee yhdellä Mailbox-palvelimella ja passiiviset kopiot muilla Mailbox-palvelimilla. Optimoidussa tilanteessa kopiot ovat useassa eri palvelinkeskuksessa.

Edge Transport -rooli on ollut aiemmissa Exchange-järjestelmissä tärkeä, vaikkakaan ei pakollinen, koska sen voi toteuttaa jollakin kolmannen osapuolen tuotteella. Roolia ei ole tuotu Exchange Server 2013:een, mutta roskapostin suodatusominaisuudet kuitenkin löytyvät. Käytännössä paras ratkaisu on asentaa joko Exchange 2010 Edge -palvelin tai joku muu roskapostin suodatustuote verkon DMZ-alueelle. Esimerkkejä Edge-palvelimista ovat F-Securen Messaging Security Gateway sekä Trend Micron Interscan Messaging Security.

3.2 **Roolien vikasietoisuus**

CAS Array on useamman Client Access -palvelimen kokonaisuus, jonka edessä on yleensä Kuormantasaaja (Load Balancer). Kuormantasaaja jakaa asiakasyhteydet tasaisesti eri palvelimien välillä. Kuormaa jaetaan ”Round Robin” -tyyppisesti eli asiakasyhteydet vuorotellen jokaiselle Client Access -palvelimelle. Tasaisen kuorman lisäksi konfiguraatio havaitsee, jos yksi Arrayn jäsenistä vikaantuu ja jakaa sen jälkeen liikenteen muiden toimivien palvelimien välillä. Yksinkertaisimmillaan CAS Array voidaan toteuttaa ilman Kuormantasaajaa DNS-tietueilla ”Round Robin” -metodilla, mutta konfiguraatio ei ole vikasietoinen.

Mailbox -palvelimet voidaan konfiguroida muodostamaan Database Availability Group eli tietokannan käytettävyysryhmä, jolloin postilaatikkotietokannan aktiivinen kopio on yhdellä palvelimella ja reaaliaikaisesti päivittyvä passiivinen kopio yhdellä tai useammalla Mailbox-palvelimella. Ideana on, että jos aktiivinen kanta vikaantuu, järjestelmä aktivoi automaattisesti yhden passiivisista kopioista, ja on näin ollen vikasietoinen järjestelmä. Enimmillään tietokannan kopioita yhdessä käytettävyysryhmässä voi olla 16 kappaletta.

3.3 **Riippuvuudet**

Exchange Server 2013 tarvitsee lukuisan määrän muita teknologioita toimiakseen.

Luvussa 3.2 mainitut Exchange-roolit asennetaan Windows-palvelimille. Näitä ei pidä sekoittaa Windows-palvelimien valmiisiin rooleihin, jotka asennetaan palvelimen hallinnasta ”Add roles and features”. Exchange Server 2013 -sovellus ladataan Microsoftin verkkosivulta. Asennuksen aikana valitaan, kumpi rooli asennetaan vai asennetaanko kumpikin rooli samalle palvelimelle. Käyttöjärjestelmän täytyy olla Windows Server 2012 R2, Windows Server 2012 tai Windows Server 2008 R2 with Service Pack 1 (SP1) (Microsoft 2016). Exchange Server 2013 voidaan asentaa joko fyysiselle palvelinlaitteistolle tai virtuaaliselle alustalle tietyin reunaehdoin. Exchange Server ei tue virtualisoinnissa yleisesti käytettyjä Snapshot-varmistuksia.

Exchange Server 2013 vaatii toimiakseen Active Directoryn, jonne tallennetaan järjestelmän asetukset. Samalla Active Directory luvittaa Exchangen käytön käyttäjille ja operoinnin ylläpitäjille. Exchangen-infrastruktuurin asennus tekee suuria muutoksia Active Directoryyn. Active Directoryn toimialueen hallintapalvelinten eli Domain Controllereiden tulee olla asennettuna vähintään Windows Server 2003 SP2 -tai uudemmalle käyttöjärjestelmälle. Active Directory metsän ”Forest Functional Level” täytyy olla vähintään Windows Server 2003 Forest Functional Level tai uudempi. (Microsoft 2016.) Myös Active Directoryn Schema Master -palvelimen tulee olla Windows 2003 tai tuoreempi.

Jos Exchange-organisaatio levittäytyy useammalle kuin yhdelle Active Directory Sitelle eli useampaan fyysiseen sijaintiin, tulisi jokaisella Sitellä olla nopea yhteys Global Catalog -palvelimelle, joka toimii tavallaan Active Directoryn tietokannan kopiona. Vaihtoehtoisesti jokaiselle Sitelle asennetaan Global Catalog -palvelin. (Shields, 2013).

Sähköpostin reititykseen internetin kautta käytetään MX-tietueita, jotka sisältävät julkisen IP-osoitteen Exchange-järjestelmään. Tämä mahdollistaa sähköpostin liikkumisen julkisessa verkossa organisaatioiden välillä. Asiakkaat eli sähköpostipalvelun käyttäjät löytävät Exchange-palvelimet sisä- ja ulkoverkossa DNS-tietueiden (a-tietue) perusteella. TXT- ja SPF-tietueet kertovat internetissä muille, mitkä IP-osoitteet ovat sallittuja osoitteita lähettämään sähköpostia tietystä toimialueesta. Näiden tietueiden tarkoitus on puhtaasti vähentää roskapostittajien määrää sekä erityisesti niin kutsuttua Email Address Spoofingia. Email Address Spoofingilla tarkoitetaan sitä, että joku voisi lähettää asiakkaan nimissä sähköpostia väärentämällä lähettäjän tiedot.

Sähköpostien välitys käyttäjältä toiselle perustuu verkkoyhteyksiin. Exchange-palvelimilla on oltava verkkoyhteys ja suojattu internetyhteys palomuurien ja Edge-palvelimien kautta. Sisäverkkoyhteyksien pitää toimia toimialueen ohjauskoneille sekä DNS- ja DHCP-palveluihin.

Varsinaista palvelinta tai käyttöjärjestelmä-konfiguraatiota ei tarvitse varmistaa, sillä asetukset tallentuvat Active Directoryyn. On kuitenkin hyvä varmistaa käytössä olevat sertifikaatit ja niiden Private Keyt toisaalle, kuten Certification Authority -palvelimelle.

Exchange Server 2013 -sähköpostitietokannat tukevat Exchange-aware VSS -teknologiaan perustuvia varmistuksia. Toisin sanoen varmistusohjelmiston täytyy tukea Exchange-tietokantoja ja osata typistää tietokantojen lokitiedostoja tarvittaessa. Microsoftin VSS- eli Volume Shadow Copy -teknologia sallii kirjoittamisen kantaan varmistuksenottohetkellä, jolloin varmistusajankohtana ei tule palvelulle käyttökatkoa. Shadow Copy tarkoittaa myös tietyn hetken tilanteen tallentamista. (Cunningham & Higginbotham 2016, 214.)

3.4 **Suositeltu arkkitehtuuri**

Exchange Server 2013 Preferred Architecture eli suositeltu arkkitehtuuri on Exchange-järjestelmän kehitystiimin oma näkemys siitä, miten Exchange-sähköpostiympäristö pitäisi asentaa. Suositeltu arkkitehtuuri on suunniteltu optimoiduksi ratkaisuksi, joka ei ole välttämätön, mutta sitä kannattaa noudattaa omat resurssit huomioiden.

Suositellun arkkitehtuurin idea on muuttaa ympäristö ennakoivaan toipumiseen. Kun esimerkiksi tietokannassa ilmenee vikatilanne, järjestelmä osaa itse aktivoida toisen tietokannan.

Tällainen ratkaisu automatisoi ylläpidon useissa ongelmatilanteissa, poistaa lähes kokonaan palvelun katkot sekä tarpeen varmistuspalveluille, kuten nauhavarmistukset. Näin ollen ylläpito yksinkertaistuu ja helpottuu.

Microsoft käyttää omassa Exchange Online -pilvipalvelussa suositeltua arkkitehtuuria, eikä omien sanojensa mukaan ota perinteisiä varmistuksia ollenkaan tietokannoista. Suositellun arkkitehtuurin huono puoli on sen kustannukset. Suomen kokoisessa maassa on vai muutama yritys, jolla on useampi, fyysisesti erillinen palvelinkeskus.

Suositeltu arkkitehtuuri ottaa kantaa seuraaviin asioihin suunniteltaessa sähköpostiympäristöä:

1. Nimiavaruus

DNS-nimipalvelussa suositellaan käytettäväksi niin kutsuttua Unbound-mallia, jossa nimiavaruus suunnitellaan siten, että käytössä on yksi nimiavaruus jokaiselle asiakaspuolen protokollalle, joka ohjaa liikennettä vähintään kahdelle erilliselle palvelinkeskukselle tasapuolisesti kuormantasausprotokollia käyttäen.

2. Palvelinkeskus

Exchange-ympäristö asennetaan vähintään kahteen palvelinkeskukseen, jotka sijaitsevat fyysisesti eri paikoissa. Näiden välille konfiguroidaan nopea ja pieni latenssinen yhteys.

3. Palvelin

Helppouden ja vikatilanteiden skaalautuvuuden vuoksi sähköpostijärjestelmä asennetaan fyysisille palvelimille, samalla pyritään välttämään virtuaalisten palvelinten käyttöä. Palvelimia voi olla useita, mutta Exchangen kaksi roolia asennetaan aina samalle palvelimelle. Tämän tarkoitus on helpottaa ylläpitoa. Käyttöjärjestelmä, Exchangen binäärit, lokit ja transport-tietokanta konfiguroidaan käyttämään kahden levyn RAID-1 -levyjärjestelmää. Exchangen postilaatikko-tietokannat asennetaan JBOD-levyjärjestelmään, joka on suhteellisen edullista ja helppoa ylläpitää.

4. Tietokannan käytettävyysryhmä

Database Availability Group konfiguroidaan jakautumaan useamman palvelinkeskuksen kesken. Useamman DAGin ympäristössä tietokantojen sekä aktiiviset että passiiviset tietokantakopiot jaetaan myös useamman palvelinkeskuksen kesken. Palvelinkeskusten tulee olla identtiset, erityisesti levykonfiguraatiossa. DAGin Witness Server asennetaan palvelinkeskukseen, jolla ei ole DAGin tietokantakopioita. Witness Server mahdollistaa automaattisen failoverin siinä tilanteessa, että kokonainen palvelinkeskus vikaantuu. Witness Serverin tehtävä on seurata tietokannan aktiivisen kopion Heart Beatia. (Smith 2014.)

3.5 **Exchange Native Data Protection**

Exchangen Native Data Protection on riippuvainen suositellusta arkkitehtuurista, ja se pohjautuu siihen ajatukseen, että perinteisistä varmistuspalveluista päästään eroon käyttämällä Exchangen omia komponentteja. (Microsoft 2016.)

Native Data Protectionissa käytettävät ominaisuudet, joiden vuoksi perinteisiä varmistusteknologioita, kuten esimerkiksi nauhavarmistuksia, ei tarvita:

1. Database Availability Groups (Tietokannan käytetävyysryhmät)

Vähintään kolme jäsentä Database Availability Groupissa, mielellään eri palvelinkeskuksissa (Cunningham & Higginbotham 2016, 212). Yksi aktiivi-

nen kopio, yksi passiivinen kopio ja yksi File Share Witness, joka havaitessaan liian ison poikkeavuuden antaa passiiviselle tietokannalle käskyn aktivoitua (Shields, 2013).

2. Single Item Recovery

Mahdollisuus palauttaa käyttäjän poistama kalenterimerkintä, sähköposti tai muu sähköpostilaatikosta poistettu kohde riippumatta siitä, mitä käyttäjä sille on tehnyt. Oletuksena asetus DeletedItemRetention eli aika jonka sisällä kohde voidaan palauttaa postilaatikkoon, on 14 päivää, mutta sitä voidaan kasvattaa esimerkiksi 365 päivään. Palautus on nopeaa ja tapahtuu loppukäyttäjän sähköpostisovelluksella. (Cunningham & Higginbotham 2016, 213.)

3. Lagged Database Copy

Lagged Database Copy on DAGin yksi jäsen, jota päivitetään ennalta määritetyllä viiveellä. Viive voi olla maksimissaan 14 päivää. Näin ollen, jos aktiivinen tietokanta vikaantuu ja vika vaikuttaa myös passiivisiin kopioihin, voidaan tilanne korjata ottamalla käyttöön Lagged Database Copy.

4. Recovery Database

Recovery Database on tietokanta, joka voidaan luoda palautuksia varten. Tietokantaan voidaan palauttaa kopio jostakin tuotannosta olevasta tietokannasta ja palautuksen jälkeen Recovery Databasesta voidaan tarvittaessa noutaa vanhoja postilaatikkoja ja Single Item Recovery ajan ylittäneitä postilaatikon kohteita, kuten sähköpostit tai kalenterimerkinnät. (Cunningham & Higginbotham 2016, 213.)

5. In-Place Hold

In-Place Hold on ominaisuus, jonka ylläpitäjä voi asettaa yksittäiseen postilaatikkoon. Käytännössä se tarkoittaa sitä, että poistetut kohteet eivät häviä postilaatikosta edes edellä mainitun DeletedItemRetentionin jälkeen, vaan pysyvät postilaatikossa. Alun perin ominaisuus kehitettiin oikeudenkäyntejä varten ja sitä kutsuttiin Litigation Holdiksi. Ominaisuuden myötä sähköpostiviesti ei oikeasti katoa postilaatikosta, vaikka käyttäjä luulee poistaneensa viestin. (Elfassy 2014, 45.)

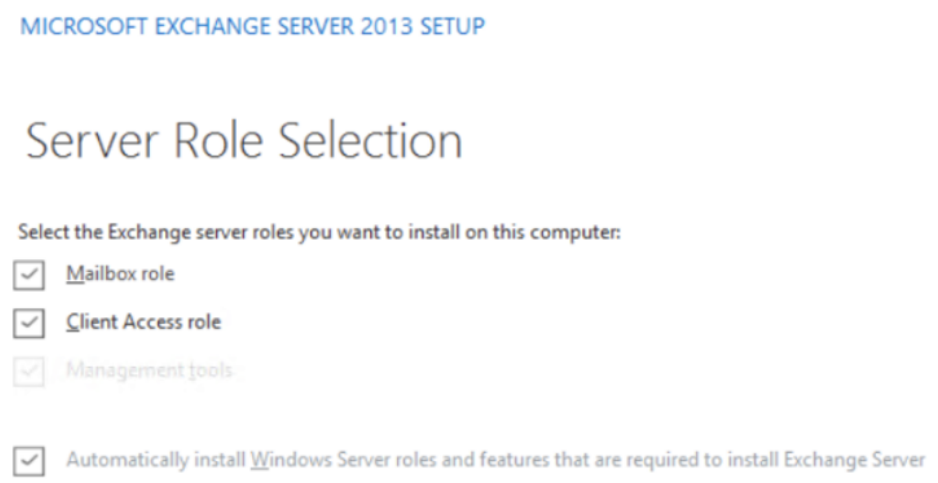
3.6 **Asennus ja konfiguraatio**

Exchange Server 2013 -asennusmedia ladataan Microsoftin verkkosivulta https://www.microsoft.com/en-gb/evalcenter/evaluate-exchange-server-2013. Lataus on automaattisesti purkautuva tiedosto. Puretusta mediakansiosta löytyy Setup.exe -tiedosto, jolla käynnistetään asennus. Asennus tehdään Active Directory -toimialueelle liitetylle Windows-palvelimelle, jolla on kiinteä IP-osoite.

Ensimmäiseksi asennus tarkistaa internetistä mahdolliset päivitykset, ja vaikka kohdan voi ohittaa, on erittäin suositeltavaa tietoturvan kannalta

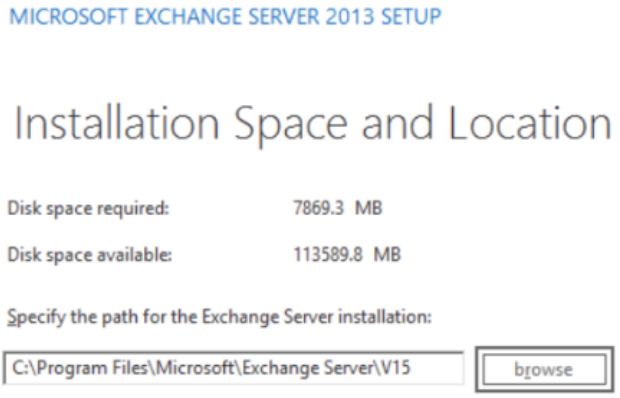
ladata tarjolla olevat päivitykset. Asennuksen jälkeen sähköpostijärjestelmä on kuitenkin heti käytettävissä ja tietoturvasta on huolehdittava.

Seuraavaksi valitaan asennettavan Exchange-palvelimen roolit (Kuva 3). Pienissä ympäristöissä asennetaan sekä Mailbox- ja Client Access -rooli yhdelle palvelimelle. Suuremmissa ympäristöissä ja niissä toteutuksissa, joissa roolit eriytetään, asennetaan ensin Mailbox-roolin palvelin ja sen jälkeen Client Access-palvelin.



Kuva 3. Palvelinroolin valinta.

Seuraavaksi valitaan kohde, johon itse Exchange-sovellus asennetaan (Kuva 4).



Kuva 4. Asennuksen sijainti.

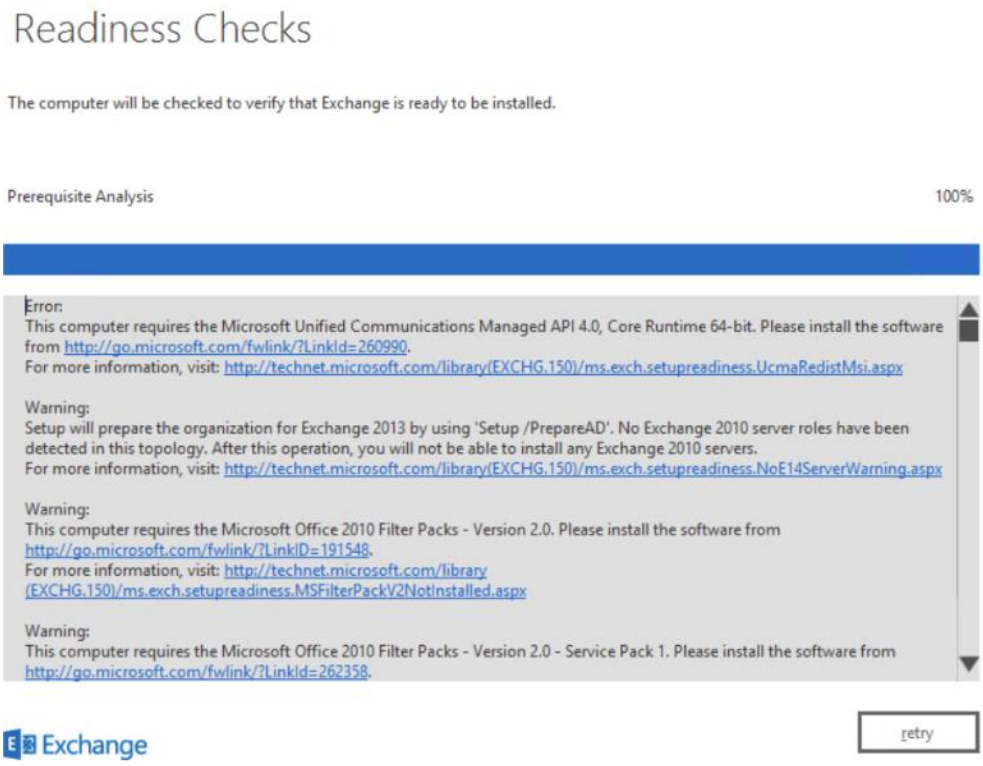
Vaikka asennus tarjoaa sovelluksen oletussijainniksi samaa levyä, jolla on käyttöjärjestelmä, on suositeltavaa asentaa Exchange eri levylle. Tämä valinta ei ole kuitenkaan ehdoton. Asennuksen sijainti vaikuttaa muun muassa i/o -suorituskykyyn eli siihen, kuinka nopeasti järjestelmä kykenee kirjoittamaan ja lukemaan dataa.

Kuva 5. Organisaatio ja Split Permissions.

Seuraavaksi valitaan sähköpostiorganisaatiolle nimi, jolla ei ole toimivuuden kannalta kovin suurta merkitystä(Kuva 5). Nimen alla oleva ”Apply Active Directory split permissions...” valitaan, jos sähköpostijärjestelmän asentajalla ei ole toimialueen ylläpitäjätason oikeuksia vaan Exchangen ylläpidolle varatut järjestelmävalvojan oikeudet.

Seuraavaksi asennus kysyy, disabloidaanko haittaohjelmien skannaus, joka voidaan valita, jos ympäristössä on jo toinen palvelu, joka suodattaa haittaohjelmia. Muussa tapauksessa ominaisuus kannattaa pitää päällä.

Lopuksi, ennen varsinaista asennusta, sovellus tekee Readiness Checks-testin (Kuva 6):

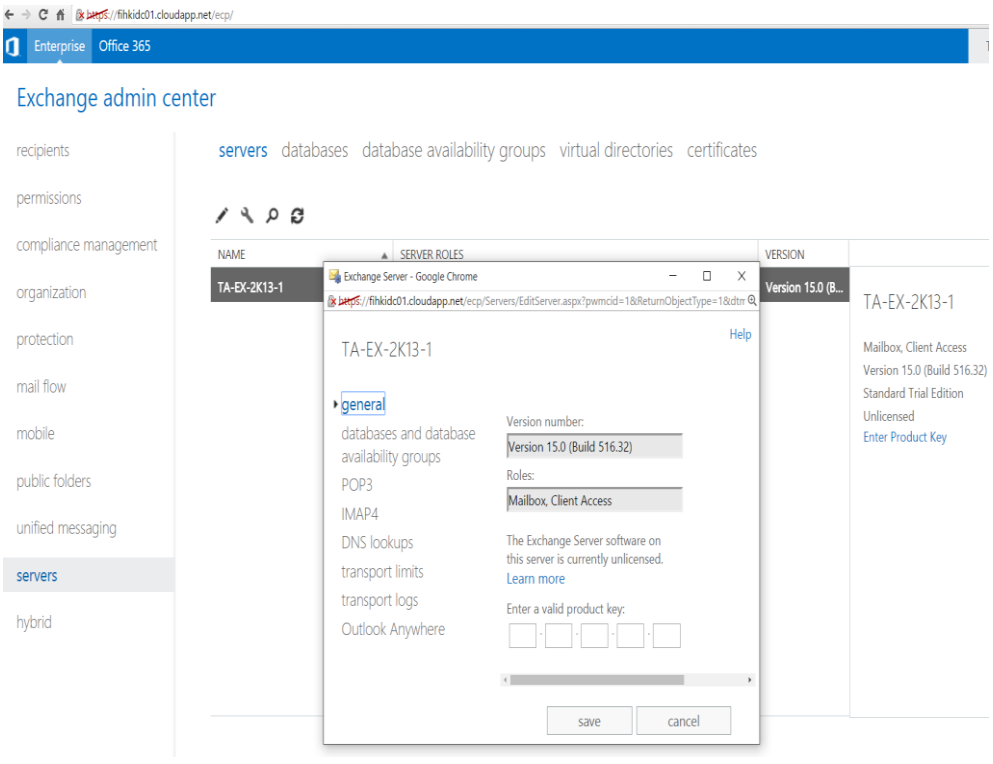


Kuva 6. Readiness Checks -testin tulokset.

Testi tarkistaa Active Directory -ympäristön ja -palvelimen valmiudet Exchange-palvelimeksi. Testin tuloksista näkee, mitä ongelmia tai esteitä järjestelmän palveluille testin aikana on ilmennyt. Useimmat varoitukset liittyvät pieniin ohjelmiin, jotka tarvitaan toimivuuden kannalta ja ne asentuvat valittaessa varoituksesta asennusvaihtoehto. Kuvassa 6 on hyvin yleisiä virheilmoituksia, joita tulee Windows-palvelimella. Tässä tapauksessa asennetaan testin perusteella muun muassa MS Unified Communications Managed API 4.0, MS Office 2010 Filter Packs 2.0 ja sen SP1.

Asennuksen jälkeen samaan Active Directoryyn, jossa on Exchange Server 2010, ei voida asentaa enää yhtään palvelinta. Tämä on huomioitava siinä tapauksessa, jos aiotaan käyttää sitä SMTP gatewayna, koska Exchange Server 2013:ssa sitä ominaisuutta ei ole. Todennäköisesti tuotantoympäristöissä käytetään kuitenkin kolmannen osapuolen tuotetta. Asennuksen aikana tulee oikeuksiin liittyviä virheilmoituksia, mikäli käyttäjä, joka asennuksen tekee, ei ole Enterprise Admin tai Schema Admin. Asennuksen yhteydessä tehdään erittäin suuria muutoksia AD:n Schemaan, ja niitä ei voida asennuksen jälkeen peruuttaa. Toisin sanoen asentajan tunnuksen pitää kuulua joko Enterprise Admins-, Domain Admins- tai Schema Admins -ryhmään.

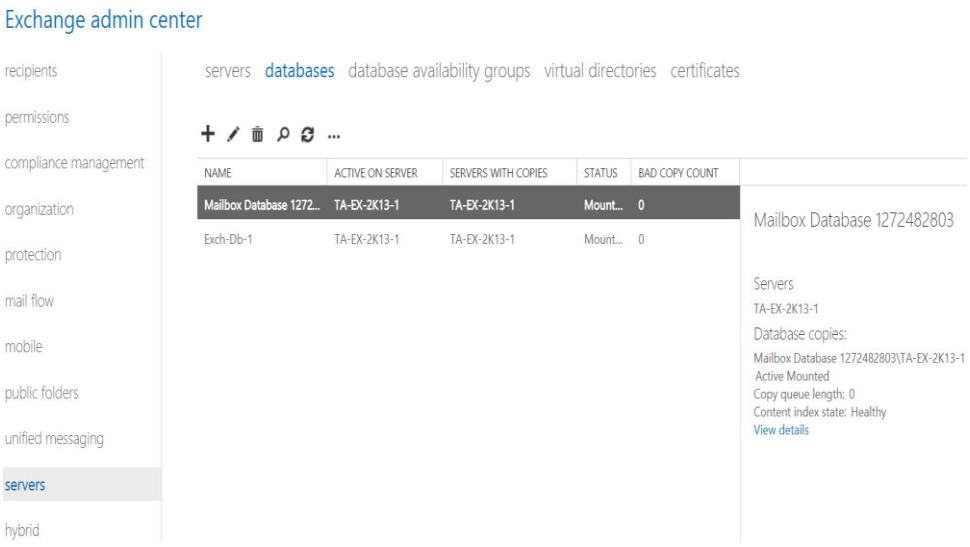
Asennuksen jälkeen sähköpostijärjestelmän hallinta tapahtuu internet-selaimella ja Exchange Management Shellillä, joka on Windows Powershellin moduuli. Siinä on merkkipohjainen hallinta ja se asentuu Management Tools -asennuksella. Selainhallinta aukeaa asennuksen jälkeen sähköpostipalvelimen internet-selaimella osoitteessa https://localhost/ecp. Tätä hallintaa kutsutaan Exchange Admin Centeriksi.



Kuva 7. Lisenssin syöttö sovellukselle selainhallinasta.

Jos asennettava palvelin ei ole testipalvelin vaan tuotantoon tuleva palvelin, on sille käytävä syöttämässä lisenssiavain. Tämän voi tehdä Exchange Admin Centerissä (Kuva 7).

Toinen tärkeä ensivaiheen toimenpide on käydä poistamassa Exchange-asennuksen luoma sähköpostilaatikkotietokanta, joka on yleensä samassa kansiossa Exchange-binäärien kanssa ja nimetty pitkällä numerosarjalla (Kuva 8).



Kuva 8. Tietokantojen hallinta verkkoselaimella.
Käyttöön tulevat tietokannat kannattaa nimetä loogisesti, esimerkiksi mdb1, mdb2 jne. Ne luodaan tietokannoille dedikoiduille levyosioille.

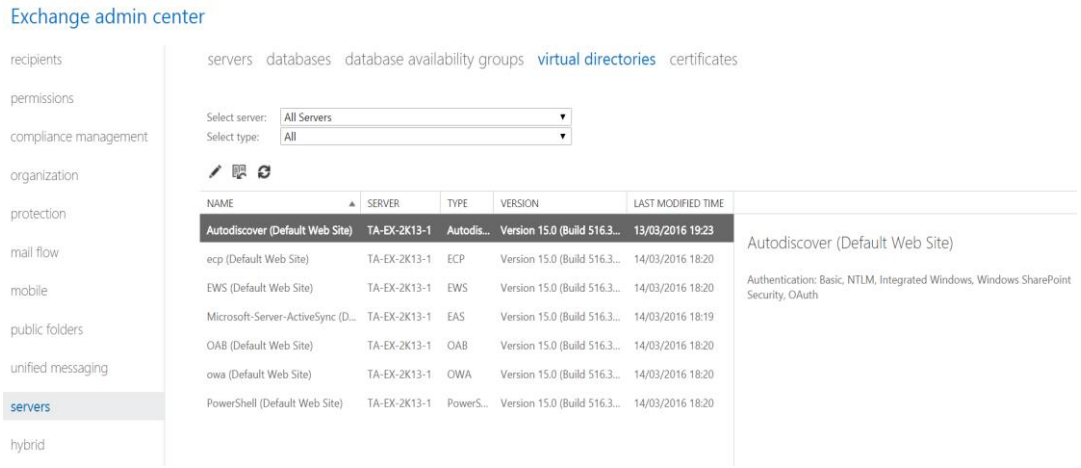
Seuraavaksi DNS-palveluun lisätään yleiset Exchangen osoitteet (Taulukko 1).

Taulukko 1. DNS-tietueet. Esimerkki ympäristöstä, jossa toimialueen nimi on asiakas.fi, Exchangen eri protokollat sidotaan IP-osoitteisiin A- ja MX -tietueilla.

Nimi	**Tyyppi**	**Data**
Mobimail.asiakas.fi	A	195.234.136.33
Autodiscover.asiakas.fi	A	195.234.136.33
Webmail.asiakas.fi	A	195.234.136.185
Mail.asiakas.fi	A	195.234.136.34

mail.asiakas.fi	A	195.234.136.35
asiakas.fi	MX	Mail.asiakas.fi

DNS-asetusten jälkeen Exchangen virtuaaliset hakemistot on konfiguroitava (Kuva 9). Konfigurointi kertoo, mistä URL:sta tietty palvelu vastaa.



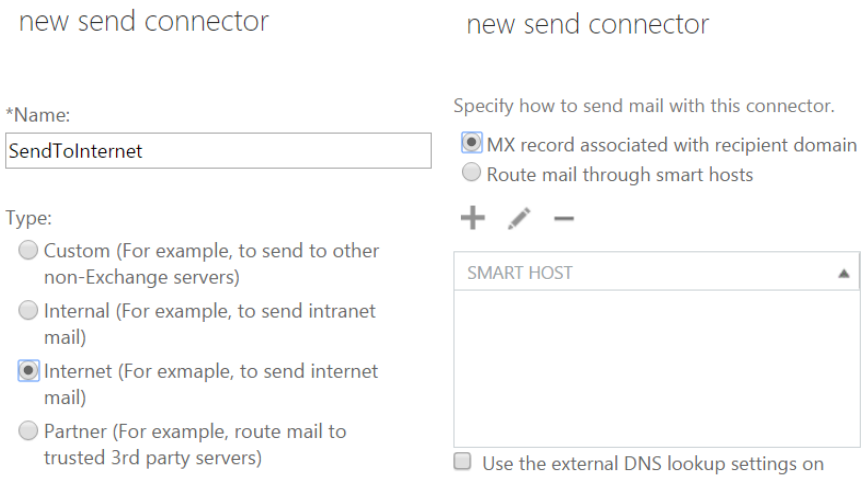
Kuva 9. Virtuaalihakemistojen konfiguraatiot.

Kannattaa huomioida, että muutosten tekeminen Exchangen Virtual Directoryyn on sama kuin tekisi ne IIS-palvelimen osoitteisiin. IIS -palvelu asentuu Exchangen myötä palvelimelle ja on Microsoftin Internet-palvelinsovellus.

Kuva 10. Virtuaalihakemiston asetus Management Shellillä.

Esimerkissä asetetaan Exchange Management Shellillä Autodiscover -osoite, jolla Outlook-asiakkaat löytävät automaattisesti sähköpostijärjestelmän (Kuva 10).

Tässä vaiheessa organisaation sisäinen sähköposti toimii.
Jos halutaan lähettää ja vastaanottaa myös organisaation ulkopuolista sähköpostia, on MX-tietueiden ja Edge-palvelimen lisäksi konfiguroitava lähetysyhdistin (Send Connector) ja vastaanottoyhdistin (Receive Connector).



Kuva 11. Lähetysyhdistimen luonti.

Luodaan MX-tietueeseen perustuva lähetysyhdistin (Kuva 11). Mikäli Internetin ja Exchange- palvelimen välissä on aiemmin mainittu Edge tai SMTP Gateway -palvelin, valitaan ”Route mail through smart hosts” ja lisätään Edge -palvelimen osoite.

4 TOIPUMISSUUNNITELMA

Varsinainen toipumissuunnitelma on liitteessä I. Toipumissuunnitelma on luovutettu asiakkaalle. Asiakasorganisaation henkilöt ovat käyneet suunnitelman läpi, ja hyväksyneet sen pienillä muutosehdotuksilla. Ehdotukset koskivat muun muassa vastaanottoyhdistintä, jota ei enää käytetty, mutta joka oli edelleen konfiguroituna palveluun. Asiakkaan mielestä sitä ei pitäisi dokumentoida, mutta jätin sen Toipumissuunnitelmaan, koska sitä ei ole vielä poistettu palvelusta.

Toipumissuunnitelmaa alettiin valmistella valmiille pohjalle, jota käytetään kaikissa toipumissuunnitelmissa, joita Elisa Appelsiini Oy tuottaa. Valmiissa pohjassa ovat seuraavat osiot:

- Versionhallinta
- Toipumissuunnitelmasta vastaavat henkilöt
- Palvelukokonaisuuden eri osista vastaavat yritykset
- Yhteystiedot
- Palvelutaso
- Ympäristön kuvaus ja konfiguraatio
- Vikatilanteet
- Ongelman rajoittamistoimet

4.1 **Versionhallinta**

Dokumenttia saattaa muokata useampi henkilö projektin aikana, joten kaikki lisäykset tai muutokset on dokumentoitava versionhallintataulukkoon (Taulukko 2).

Taulukko 2. Esimerkki Versionhallinnasta

Versionumero	**Päivämäärä**	**Muuttaja**	**Selite / Muutos**	**Tila**
0.1	21.7.2016	Projektipäällikkö	Dokumentin luonti	Draft
0.2	14.10.2016	Andelin	Toipumismenetelmien kuvaus	Draft
0.3	21.10.2016	Andelin	Toteutusdokumentaation lisäys	Draft
0.4	22.11.2016	Projektipäällikkö	Yleistietojen tarkennus	Draft
0.5	2.12.2016	Andelin	Sisäinen katselmointi	Alustava versio valmis

1.0	21.12.2016	Andelin	Perustietojen korjaus	Asiakkaan 1. katselmointi

4.2 Yhteystiedot ja yhteistyökumppanit

Toipumissuunnitelmasta vastaavat henkilöt on listattu lähinnä tiedoksi asiakkaalle niistä henkilöistä, jotka dokumentaation tuottivat. Palvelusta vastaavat -listassa on eritelty palvelukokonaisuudesta vastaavat tahot.

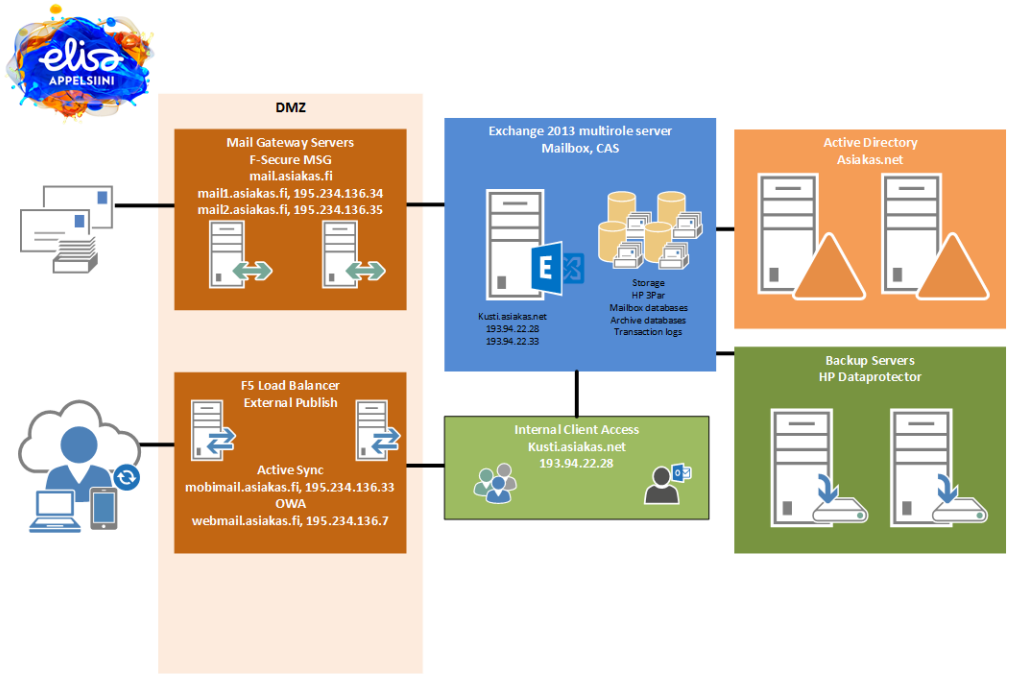
Responsible on suoritusvastuullinen taso, joka tarkoittaa käytännössä järjestelmän ylläpitäjää. Accountable on palvelun omistaja tai loppukäyttäjään nähden palvelusta vastaava taho. Consulting on esimerkiksi ylitsepääsemättömässä ongelmatilanteessa neuvova taho. Informed on taho, jota tiedotetaan muutoksista ja palvelupoikkeamista.

Esimerkiksi verkko on olennainen osa sähköpostijärjestelmän toimivuuden kannalta. Verkkoa ylläpitää Cygate (Responsible) ja verkosta vastaa asiakas (Accountable). Cisco on neuvoja, koska verkkolaitteet tulevat Ciscolta ja jos verkkoon tehdään muutoksia, on Elisa Appelsiinia tiedotettava (Informed). Tarkemmat yhteystiedot on listattu toipumissuunnitelman päädokumentissa, joten niitä ei ole ollut tarpeellista lisätä sähköpostijärjestelmän toipumissuunnitelmaan.

4.3 Palvelutaso

Palvelutaso eli Service Level Agreement on Elisa Appelsiinin ja asiakkaan välillä sovittu palvelun vaatimustaso. Palvelutasolle on sopimuskohtaisesti sovitut mittarit, joilla mitataan palvelun käytettävyyttä ja saatavuutta. Tähän järjestelmään on sovittu 24/7-palvelutaso ja käytettävyystavoitteeksi 99,9 %, joka tarkoittaa 15 minuutin reagointiaikaa Elisa Appelsiinilla ongelmatilanteessa ja neljän tunnin ratkaisuaikaa ongelmille. Ennalta sovitut huoltokatkot, kuten kuukausittaisten Microsoft-päivitysten asennukset, eivät vaikuta käytettävyystavoitteeseen. Käytettävyys ei myöskään koske yksittäistä palvelun komponenttia tai palvelinta, vaan koko sähköpostipalvelua.

4.4 Ympäristön kuvaus



Kuva 12. Sähköpostijärjestelmä ylätasolla.

Sähköpostijärjestelmä koostuu kahdesta SMTP Gateway -palvelimesta, jotka sijaitsevat verkon reunalla DMZ-alueella (Kuva 12). DMZ-alueella on myös kuormanjakaja, joka arkkitehtuurikuvan mukaan jakaa verkkokuormaa ulkoverkossa oleville ActiveSync- eli mobiililaitteille ja Verkkoselainta käyttäville OWA-asiakkaille. Varsinainen Exchange Server 2013 -palvelin sijaitsee sisäverkossa, eikä asiakas ole kokenut tarpeelliseksi kahdentaa tai toteuttaa palvelua useammalla palvelimella. Exchange-palvelin käyttää sisäverkon Active Directory -palvelua eli Microsoftin aktiivihakemistoa käyttäjien tunnistamiseen ja järjestelmän konfiguraation tallentamiseen. Sähköpostitietokannat varmistetaan perinteisellä varmistuspalvelulla, joka sijaitsee asiakkaan sisäverkossa sille määritellyllä palvelimella.

4.5 Konfiguraatio

Sisäiseen DNS-palveluun on konfiguroitu a-tietueet, joilla löytyy palvelin nimellä ja Autodiscovery-palvelu, joka auttaa sähköpostiasiakkaita löytämään palvelun. Esimerkkinä tästä voidaan pitää tilannetta, jossa käyttäjä on kirjautunut työasemalleen sisäverkossa käyttäjätunnuksellaan ja käynnistää Outlook-sähköpostisovelluksen. Autodiscover-palvelu helpottaa käyttäjän sähköpostiprofiilin asennusta jopa siinä määrin, että se vaikuttaa automaattiselta.

Ulkoiseen DNS-palveluun on konfiguroitu mail.asiakas.fi a-tietue, asiakas.fi MX-tietue ja Autodiscover- sekä mobimail.asiakas.fi a-tietue. Mail.asiakas.fi auttaa löytämään asiakkaan sähköpostipalvelun internetistä käsin. MX-tietue liikuttaa sähköpostiliikenteen oikeaan osoitteeseen,

Autodiscover auttaa Outlook-asiakkaita löytämään palvelun internet-yhteyden kautta ja Mobimail-osoite on tarkoitettu ActiveSync- eli mobiiliasiakkaiden osoitteeksi. MX-tietue on asetettu osoittamaan osoitteeseen mail.asiakas.fi, josta kuormaa jaetaan kummallekin F-Securen Messaging Security Gateway -palvelimelle.

Sertifikaatiksi on valittu julkiselta sertifikaatin tarjoajalta niin kutsuttu SAN-sertifikaatti, johon voidaan sitoa useampi nimi tai palvelu. Sertifikaatin tehtävä on todentaa ja suojata sähköpostipalvelua. SAN on lyhenne sanoista Subject Alternate Names, ja siihen on liitetty Exchangesta seuraavat nimet tai osoitteet: mobimail.asiakas.fi, palvelimennimi. asiakas.net, autodiscover.asiakas.fi, mail.asiakas.fi, asiakas.fi, asiakas.com sekä tytäryhtiöiden osoitteita. Exchangessa sertifikaatti on sidottu SMTP-, IMAP-, POP- ja IIS-palveluihin.

Sisäverkossa on käytössä myös niin kutsuttu Self-Signed -sertifikaatti, jota ei ole myöntänyt kolmas osapuoli, vaan se on luotu itse Exchange-palvelimella ja sitä käytetään vain sisäverkon asiakasyhteyksiä varten. Self-signed -sertifikaatti on sidottu vain SMTP-palveluun.

Sähköpostitietokannat ovat konfiguroitu käyttämään Mountpointeja, jotka ovat erillisiä levyjä ja asetettu näkymään G-levyn kansioina sähköpostipalvelimella. Näin ollen Microsoftin suositus tietokantojen erottamisesta käyttöjärjestelmästä toteutuu, ja sähköpostitietokannat ovat omilla levyillään. Lokitiedostokansiot ovat myös konfiguroitu käyttämään Mountpointeja. Kansioiden täytyy myös olla erillisillä levyillä, irrallaan tietokannasta ja käyttöjärjestelmän tiedostoista. Esimerkkinä voidaan tarkastella sähköpostitietokantaa MDB10, jonka sijainti on g-levyllä, Mountpoints-kansion MDB10-alikansiossa. Saman tietokannan lokitiedostot ovat Mountpoints-kansion alikansiossa MDB10Logs-alikansiossa.

Sähköpostijärjestelmä varmistetaan perinteisellä HP Data Protector -varmistusjärjestelmällä varmistusnauhoille. Sähköpostitietokantojen täysi varmistus suoritetaan päivittäin klo 15 ja kuukausittain, joka kuun 1. päivä klo 15. Eroina päivittäisten ja kuukausittaisten varmistusten välillä on niiden säilytysaika.

4.6 **Transport-asetukset**

Exchangen yleiset Transport-asetukset sisältävät määritykset sähköpostin suurimmalle mahdolliselle koolle. Vastaanotettaessa ja lähetettäessä saa sähköposti olla suurimmillaan 51 200 kilobittiä liitteineen. Suurin mahdollinen vastaanottajien määrä yksittäisellä sähköpostilla saa olla 5000.

Hyväksyttyjä toimialueita Exchangessa on asiakas.fi, asiakas.com ja muutama tytäryhtiön osoite. Näihin osoitteisiin vastaanotetaan sähköpostia. Huomattavaa näissä on esimerkiksi se, että sisäverkon asiakas.net-toimialuetta ei käytetä hyväksyttynä toimialueena. Sillä ei myöskään ole MX-tietuetta julkisessa DNS:ssä. Se on perustettu vain Active Directoryn hallintaa varten. Sisäverkon asiakas.net-toimialueeseen voidaan kuitenkin

liittää muita toimialueita, jotka taas voivat vastaanottaa sähköpostia, joten se tehdään edellä mainituilla hyväksytyillä toimialueilla.

Sähköpostiosoitteen käytännöt määrittelevät, minkälainen sähköpostiosoite luodaan Active Directory -käyttäjälle automaattisesti, kun hänelle luodaan sähköpostilaatikko. Sähköpostiosoitteen muoto on seuraava:

smtp:%rÄA%rÖO%rÅA%räa%röo%råa%g.%i.%s@asiakas.com
SMTP:%rÄA%rÖO%rÅA%räa%röo%råa%g.%i.%s@asiakas.fi

Huomattavaa on, että käyttäjällä voi olla useampia sähköpostiosoitteita. Osoite, jonka edessä isoilla kirjailla kirjoitettu SMTP on oletusvastaanotto-osoite. @-merkin edessä olevat kirjaimet tarkoittavat yksinkertaistettuna sitä, että otetaan huomioon skandinaaviset kirjaimet, jos niitä on käyttäjän nimessä, ja muutetaan ne sähköpostijärjestelmien hyväksymiin muotoihin. Esimerkiksi käyttäjä nimeltä Yrjö Äikäs saisi automaattisesti osoitteet yrjo.aikas@asiakas.com ja yrjo.aikas@asiakas.fi, joista jälkimmäinen olisi automaattisesti vastaanotto-osoite.

Lähetysyhdistimiä on kolme kappaletta. ”SMTP Internet”-osoitetta käytetään sähköpostien lähettämiseen asiakkaalta internetiin. Välittäjäpalvelimeksi on valittu F-Securen Messaging Security Gateway, jolloin sähköpostit kulkevat sen kautta. ”Test.local” on jostakin asiakkaan testistä ylimääräiseksi jäänyt yhdistin, jonka asiakas halusi poistaa toipumissuunnitelmasta. Se jätettiin toipumissuunnitelmaan, koska se on konfiguroitu järjestelmään, vaikka se ei ole käytössä. ”Securemail”-lähetysyhdistin lähettää sähköpostin salausjärjestelmään, joka lähettää asiakkaan valitsemat sähköpostit salattuina internetiin.

Vastaanottoyhdistimiä on 7 kappaletta. Näin monen vastaanottoyhdistimen tarkoitus on hallinnoida tarkemmin, millaista sähköpostidataa ja mistä peräisin olevaa liikennettä sallitaan saapuvaksi sähköpostipalvelimelle. Useimmiten vastaanottoyhdistimiä on vain muutama, joista yhdellä vastaanotetaan sähköpostia internetistä ja toisella sallitaan ne palvelimet ja palvelut, joiden annetaan lähettää sähköpostia Exchange-palvelimen kautta, esimerkiksi Sharepoint, raportointipalvelut, skannerit ja tulostimet.

Kuvaavan nimen lisäksi vastaanottoyhdistimeen määritellään Autentikointi-menetelmä, jolloin voidaan pakottaa muun muassa TLS-salaus sähköpostille tai antaa salaamattoman postin tulla läpi. Luvitetun lähettäjäryhmän (”Permission Groups”) avulla määritellään, keneltä halutaan vastaanottaa sähköpostia. Jotta internetistä voidaan vastaanottaa sähköpostia, luvitetun ryhmän tulee olla Anonymous. Tähän voidaan määritellä myös vastaanotto vain toisilta Exchange-palvelimilta, tunnistetuilta yhteistyöorganisaatioilta, joiden kanssa on Active Directory -luottosuhde tai vain ko. Exchange-organisaation käyttäjien välistä postia. Lopuksi voidaan rajatta liikenne vielä tiettyihin IP-osoitteisiin ja -portteihin.

F-Securen Messaging Security Gateway on asennettu kahdelle DMZ-alueella sijaitsevalle palvelimelle. Toinen on niin sanottu Config Master ja toinen Agent/Mail Filter. Config Master on palvelin, johon on tallennettu Gatewayn konfiguraatio ja sekin toimii Agent/Mail Filterinä. Ne suodattavat ennalta luoduilla säännöillä roskapostin ja haittaohjelmia sisältävät sähköpostiviestit. Palvelinten kautta tarjotaan loppukäyttäjille myös verkkoselainpohjainen palvelu, josta he näkevät muun muassa henkilökohtaisen roskapostikaranteenin.

4.7 Tekniset riippuvuudet

Tekniset riippuvuudet jaotellaan toipumissuunnitelmassa kahteen osaan. Niihin järjestelmiin, joista Sähköpostipalvelun toiminta on riippuvainen (Taulukko 3) ja niihin järjestelmiin, joiden toiminta on sähköpostipalvelusta riippuvainen (Taulukko 4). Kuvaukseen kuuluu myös se, mitä tapahtuu, jos palvelu on alhaalla. Esimerkiksi jos Active Directory on alhaalla tai Exchange-palvelin ei saa yhteyttä toimialueen ohjauskoneisiin, sähköpostipalvelu tai sen hallintapalvelu ei ole saatavilla.

Taulukko 3. Esimerkkejä sähköpostijärjestelmän riippuvuuksista. Otteet toipumissuunnitelmasta.

Järjestelmä	**Kuvaus**
VMware	Exchange asennettu virtuaalipalvelimelle. Sijainti VMwaressa vcenter turbo, HKI (B-sali) / Production. Jos VMware ei toimi, palvelu ei ole saatavilla. Varmistamattomia tietoja voidaan menettää.
Active Directory	Jos AD ei toimi (domain controllereihin ei ole yhteyttä), palvelu ja hallintapalvelu eivät ole saatavilla. Active Directory sisältää tiedot kaikista ympäristön käyttäjistä, sekä heille määritetyistä oikeuksista ja asetuksista. Sähköpostijärjestelmä hakee tiedot suoraan AD:sta ja se ei voi toimia, jos Active Directory on pois käytöstä. Samoin sähköpostipalvelimen asetukset tallennetaan Active Directoryyn. Jatkuva yhteys domain controlleriin (AsiakasAB.net) oltava.
DNS	Palvelu rajoittunut, ulkoisen nimipalvelun MX-tietue ohjaa sähköpostiliikennettä, A-tietueet yhdistää ulkoverkossa olevat asiakkaat sähköpostijärjestelmään. Sisäiset tietueet yhdistävät sisäverkon sähköposti asiakkaat järjestelmään.
Levyjärjestelmät ja varmistuspalvelut	Palvelin hyödyntää vmwaressa saatavilla olevia LUNeja levyosiona ja niiden tulee olla saatavilla. Varmistuspalvelu tulee olla saatavilla. HP 3Par ja HP Dataprotector
F5	Julkaisee Exchangen sähköpostipalveluita ulkoverkon käyttäjille mobiili- ja webmail –muodossa.

Seuraavaksi toipumissuunnitelmassa luetellaan ne järjestelmät ja palvelut, jotka ovat riippuvaisia sähköpostipalvelimen toimivuudesta.

Taulukko 4. Esimerkkejä järjestelmistä, jotka ovat riippuvaisia sähköpostipalvelun toimivuudesta.

Clientit	Outlook ja Outlook Web App
Lync/Skype	Kalenteritiedot
Monitoimikoneet	Skannaus sähköpostiin
Neuvotteluhuoneiden EVOKO näytöt	ews (kalenteritiedot)
Puhelinvaihteen ZyLink	ews (kalenteritiedot)

4.8 **Ennakoidut vikatilanteet**

Toipumissuunnitelman Ennakoidut vikatilanteet -osio on dokumentin tärkein osa. Siihen kuvataan yleisimmät järjestelmän vikatilanteet, jotka aiheuttavat palvelun käytön heikentymisen tai käyttökatkon (”Disaster”).

Vikatilanteet, joihin tässä toipumissuunnitelmassa on sovittu varauduttavan, ovat seuraavat:

- Palvelinongelmat
- Sähköpostitietokannan korruptoituminen
- Sähköpostitietokannan tietojen korruptoituminen

Vikatilanteen lisäksi kuvataan menetelmä, jolla kyseessä oleva vikatilanne saadaan korjatuksi. Sovimme, että menetelmät kuvataan tarkkuudella, jolla kuka tahansa palvelutarjoajan järjestelmäasiantuntija voi korjata ongelmatilanteen menetelmää käyttäen ja toipumistavoitteet huomioiden (Taulukko 5).

Taulukko 5. Sähköpostijärjestelmälle sovitut Toipumisaika- ja Toipumispistetavoitteet.

Ongelmatilanne	**Toipumisaikatavoite (RTO)**	**Toipumispistetavoite (RPO)**
Exchange-palvelimen vikaantuminen	4h	24 tuntia, Viimeisin varmistus jonka perusteella palautus on tehtävissä
Järjestelmän tietokanta korruptoitunut	4h	24 tuntia, Viimeisin varmistus jonka perusteella palautus on tehtävissä

Sähköpos-tilaatikkoja menetetty	4h	24 tuntia, Viimeisin varmistus jonka perusteella palautus on tehtävissä

Ongelmatilanteet ja toipumismenetelmät ovat liitteessä 1. Ensin kuvataan yksinkertaisesti ongelmatilanne, kuten:”Exchange-palvelin menetetty ja se ei toivu uudelleenkäynnistyksellä tai muulla yksinkertaisella toimenpiteellä”. Sen jälkeen kuvataan toipumismenetelmä:

1. Resetoi palvelimen ad-tili.
2. Asenna palvelimen käyttöjärjestelmä ja nimeä palvelin samalla nimellä kuin aikaisempikin Exchange-palvelin, kts. dokumentaatio. Palautus ei onnistu muulla nimellä. Aiemmat asetukset on tallennettu Active Directoryyn alkuperäisen palvelimen nimellä. Varmista myös, että palvelimeen liitetään samat IP-osoitteet kuin aiemmin. Jaa levyt dokumentaation levykoot ja kirjaintunnisteet huomioiden. Alla mainittu Exchange Server recovery ei onnistu, ellei levyosiot ole samalla tavalla kuin aiemmin.
3. Liitä palvelin toimialueelle.
4. Asenna tietoturvapäivitykset Wsus järjestelmän kautta.
5. Asenna ennalta vaaditut työkalut ja käyttöjärjestelmäkomponentit. Tarkat vaatimukset Microsoftin dokumentaatiosta Exchange 2013 system requirements and Exchange 2013 prerequisites

a) Aja seuraava komento Powershellissä

```
Install-WindowsFeature AS-HTTP-Activation, Desktop-Expe-
rience, NET-Framework-45-Features, RPC-over-HTTP-proxy,
RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-
Clustering-Mgmt, RSAT-Clustering-PowerShell, Web-Mgmt-
Console, WAS-Process-Model, Web-Asp-Net45, Web-Basic-
Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Brows-
ing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Log-
ging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-
Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-
Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-
Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Com-
pression, Web-Static-Content, Web-Windows-Auth, Web-WMI,
Windows-Identity-Foundation, RSAT-ADDS
```

c)Asenna .NET framework 4.5.2
d)Asenna Windows Management Framework 4.0
e)Asenna Microsoft Unified Communications Managed API 4.0, Core Runtime 64-bit

6. Avaa komentokehoite.
7. Navigoi Exchange 2013 asennusmedian sisältämään kansioon ja aja seuraava komento Setup /m:RecoverServer /IAcceptExchangeServerLicenseTerms
8. Asennuksen valmistuttua, mutta ennen tuotantoon asettamista, konfiguroi kaikki custom-asetukset, joita aiemmalla tuotantopalvelimella oli (katso yo. taulukko).
9. Uudelleenkäynnistä palvelin.
10. Palauta ja ota käyttöön tietokannat mountpointeille osion 4.2.1 mukaan.

Menetelmäkuvauksesta voidaan todeta, että se on tarkoitettu järjestelmäasiantuntijalle, joka osaa ylläpitää Windows-palvelimia. Hyvä puoli menetelmäkuvauksessa on kuitenkin se, ettei Exchange-palvelinasiantuntijaa välttämättä tarvita toipumisoperaatioon.

Ongelman rajoittamistoimet -kohdassa kuvataan ne keinot, joilla palveluntarjoajan mielestä voidaan joko kokonaan tai ainakin osittain päästä eroon mahdollisista vikatilanteista tai ainakin estää vikatilanteen aikainen palvelun käyttökatko. Esimerkiksi jos sähköpostitietokanta menetetään, ja se ei pysty tallentamaan reaaliajassa sille tulevia sähköposteja ja toipumisaikatavoite on neljä tuntia, voidaan sisääntuleva sähköpostiliikenne katkaista F-Securen Messaging Security Gatewayllä, niin että sähköpostit kasaantuvat sen tietokantaan. Vaihtoehtoisesti katkaisu voidaan myös tehdä niin, etteivät mail1.asiakas.fi tai mail2.asiakas.fi vastaanota postia, jolloin sähköpostit jäävät jonottamaan lähettäjän ympäristön sähköpostipalvelimelle. Rajoittamiskeinoihin voidaan sisällyttää kehittämisideoita, kuten liitteessä 1, jossa mainitaan, että tietokannan korruptoituminen johtaa aina tuotantokatkoon, ellei asenneta toista Exchange-palvelinta ja luoda palvelinten välille tietokannan käytettävyysryhmää.

Lopuksi kuvataan ne prosessit, joilla voidaan todeta palvelun taas toimivan ja olevan tuotantokelpoinen. Osiossa Tuotantokelpoisuuden testaaminen mainitaan, että sähköpostin lähetystä on testattava esimerkiksi sisäverkossa, sisäverkosta ulkoverkkoon sekä ulkoverkosta sisäverkkoon. Testit on suhteutettava sen hetkiseen vikatilanteeseen.

5 YHTEENVETO

Opinnäytetyössä oleva sähköpostijärjestelmän toipumissuunnitelma on laadittu yhden Exchange-palvelimen ympäristölle. Yhden palvelimen ympäristössä on hyviä ja huonoja puolia. Ylläpito on verrattain helppoa ja selkeää. Asiakas ei ole kokenut useamman palvelimen tarjoamaa korkeaa saatavuutta tai vikasietoisuutta sen arvoiseksi, että sitä kannattaisi toteuttaa.

Totta on, että Exchange Server 2013 on vakaa tuote ja oikein konfiguroituna se ei vikaannu helposti. Mutta vikaantuessaan yhden palvelimen ympäristö kokee kuitenkin aina tuotantokatkon. Toipumissuunnitelmassa kuvatuissa ongelmatilanteissa kyse on aina useamman tunnin korjaustoimenpiteistä, joiden aikana palvelu ei ole loppukäyttäjän saatavilla. Myös varmistusten saatavuus korostuu vikatilanteessa. Tietokantojen kopiot sijaitsevat vain varmistuspalvelun nauhoilla.

Jos käytössä olisi kaksi Exchange 2013 -palvelinta, jo sillä voitaisiin todennäköisesti eliminoida tuotantokatkot useimmissa tilanteissa kokonaan. Kahdella Exchange Server 2013 -palvelimella voidaan muodostaa sekä CAS-Array, että sähköpostitietokantojen käytettävyysryhmä.

Jos ympäristö olisi rakennettu Microsoftin Data Protection Plan huomioiden, voitaisiin perinteisistä varmistuskeinoista luopua ja palvelun saatavuus olisi todennäköisesti huippuluokkaa, kuten Microsoftin omassa O365:ssa. Tämänkaltainen ratkaisu on kuitenkin hyvin kallis ja vaatii useamman kuin kahden palvelinkeskuksen IT-infrastruktuurin.

Asiakas ei ole halunnut siirtää sähköpostiaan pilveen eli käytännössä O365-palveluun, sillä asiakkaalle on ensiarvoisen tärkeää, että sähköpostidata sijaitsee omissa palvelinsaleissa eikä ulkomailla. Useimmiten tällaiset toimijat ovat valtion, kuntien tai muita korkean tietoturvan omaavia organisaatioita.

Opinnäytetyötä tehdessäni havaitsin kuinka toipumissuunnitelma on hyvä dokumentaatio kuvaamaan tuotantoympäristön arkkitehtuurin, konfiguraation sekä yleisimmät vikatilanteet ja kuinka niistä toivutaan. Erityistä arvoa toipumissuunnitelma antaa asiakkaan mukaan IT-ympäristöjen auditointiin.

6 LÄHDELUETTELO

Elisa Appelsiini (2016). Asiakkaan ICT-järjestelmien toipumissuunnitelma. Sisäinen dokumentaatio. Haettu 6.3.2016 https://apaja.elisa.fi/pages/viewpage.action?pageId=895975562

Elfassy, D. (2014). *Mastering Microsoft Exchange Server 2013*. Indianapolis, Indiana: John Wiley & Sons, Inc.

Joffel, E. (2011). Infrastruktuurin jatkuvuudenhallintastrategia Appelsiini v1.0, Apaja. Elisa Appelsiini Oy. Haettu 12.1.2017 osoitteesta https://apaja.elisa.fi/download/attachments/158236807

Microsoft(n.d.). Exchange Server 2013. Haettu 8.1.2017 osoitteesta https://products.office.com/fi-fi/exchange/microsoft-exchange-server

Smith IV, R. (2013). Exchange 2013 Server Role Architecture, Technet Blogi. Microsoft. Haettu 9.1.2017 osoitteesta https://blogs.technet.microsoft.com/exchange/2013/01/23/exchange-2013-server-role-architecture

Microsoft (2016). Exchange 2013 prerequisites. Haettu 15.12.2016 osoitteesta https://technet.microsoft.com/en-us/library/bb691354(v=exchg.150).aspx

Microsoft (2016). Exchange Server Supportability Matrix. Haettu 15.12.2016 osoitteesta https://technet.microsoft.com/en-us/library/ff728623(v=exchg.150).aspx

Shields, G. (2013). Core Solutions of Microsoft Exchange Server 2013, CBT Nuggets. CBT Nuggets. Haettu 12.1.2017 osoitteesta https://www.cbtnuggets.com/it-training/microsoft-exchange-server-2013-70-341

Cunningham, P. & Higginbotham, A. (2016). *Exchange Server Troubleshooting Companion*. Published by Paul Cunningham and Andrew Higginbotham.

Smith IV, R. (2014). The Preferred Architecture. Haettu 15.2.2016 osoitteesta https://blogs.technet.microsoft.com/exchange/2014/04/21/the-preferred-architecture

Microsoft (2016). Backup, Restore, and Disaster Recovery. Haettu 20.2.2016 osoitteesta https://technet.microsoft.com/en-us/library/dd876874(v=exchg.150).aspx

Microsoft (2016). Exchange Server 2013. Haettu 13.11.2016 osoitteesta https://technet.microsoft.com/en-us/library/bb124558(v=exchg.150).aspx

TOIPUMISSUUNNITELMA LIITE I

Yleistä

Tässä dokumentissa on kuvattuna sähköpostijärjestelmän toipumissuunnitelma. Järjestelmän tuottamaa palvelua käyttää koko asiakkaan henkilöstö sekä monet sidosryhmät ja järjestelmät. Palvelun toiminta on edellytyksenä sähköpostipalveluiden toiminnalle. Palveluihin kuuluu sähköpostin välitys organisaation sisällä, organisaatiosta ulos ja internetistä sisään. Sitä käytetään lisäksi kalenteritoimintoihin kuten videoneuvottelujen järjestämiseen ja neuvotteluhuoneiden varauksiin. Henkilökohtaisten sähköpostien lisäksi järjestelmä käsittelee resurssi- ja yhteiskäyttöpostilaatikoiden viestejä.

Tämä suunnitelma koskee Exchange 2013:a (yksi palvelin) ja F-Securen MSG Gateway-järjestelmiä.

Tästä toipumissuunnitelmasta vastaavat

Nimi	Organisaatio	Asema
Asmo Tapaninen	Elisa Appelsiini	Esittää asiakkaalle toipumissuunnitelman muutokset ylätason dokumentissa kuvatun aikataulun mukaisesti
Tuomo Andelin	Elisa Appelsiini	Valvoo muutosten päätymisen dokumentaatioon
Etunimi Sukunimi	Asiakasyritys	Hyväksyy toipumissuunnitelman muutokset

Palvelusta vastaavat

Koko järjestelmä on Appelsiinin toimittama ja sen toimivuus on Appelsiinin vastuulla. *Laitteistomuutokset ympäristöön toteuttaa asiakkaan valitsema toimittaja.*

	Responsible (suoritus-vastuullinen)	Accountable (vastuussa / omistaja)	Consulting (neuvoja)	Informed (tiedotettava)
Fyysinen laitteisto pl. verkko	Elisa Appelsiini	Asiakas	HP	
Verkko	Cygate	Asiakas	Cisco	Elisa Appelsiini
Käyttöjärjestelmä	Elisa Appelsiini	Asiakas	Microsoft	

Exchange palvelut ja tie-tokanta	Elisa Appelsiini	Asiakas	Microsoft	
F-secure MSG	Elisa Appelsiini	Asiakas	F-secure	
Varmuuskopiointi	Elisa Appelsiini	Asiakas	HP	
Deltagon turvaposti	Deltagon	Asiakas	Elisa Appel-siini	

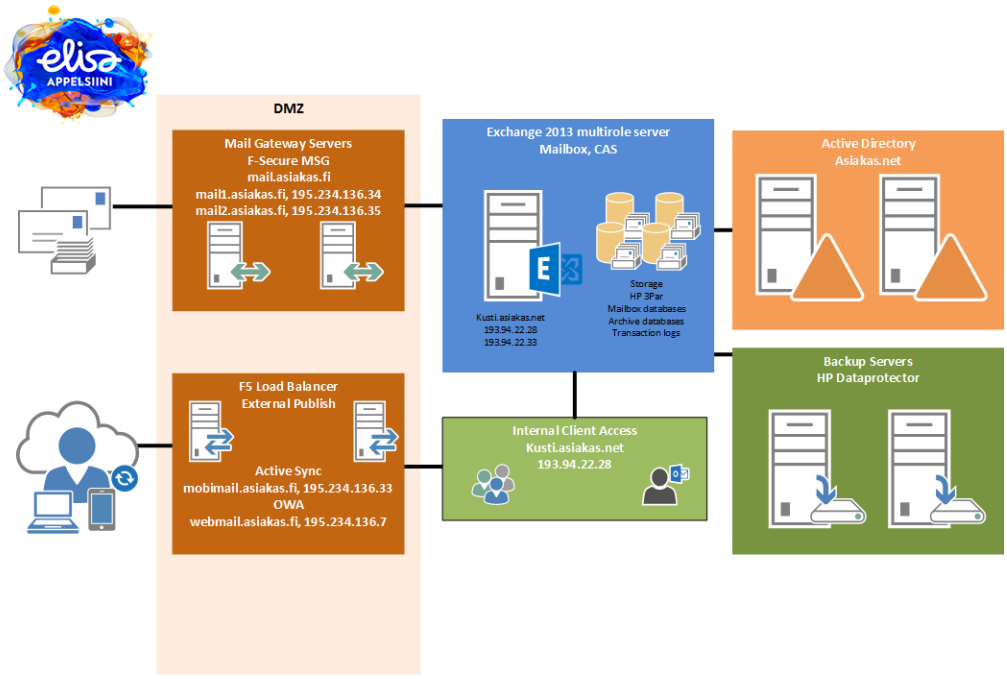
Yhteystiedot

Yhteystiedot on listattu toipumissuunnitelman päädokumentin yhtey-dessä.

Palvelutaso (SLA)

Järjestelmäkohtainen palvelutaso määritetään puitesopimuksen mukai-sesti ja järjestelmän komponenttien palvelutason perusteella. Tähän jär-jestelmään on sovittu sovellettavan palvelutasoa 24/7 ja käytettävyysta-voitteeksi on määritelty 99,9 %, joka tarkoittaa 15 minuutin reagointiai-kaa ja 4 tunnin ratkaisuaikaa. Sovitut huoltokatkot eivät ole tämän toipu-missuunnitelman tarkoittamia palvelukatkoksia. Palvelun tai järjestelmän saatavuudella tarkoitetaan koko palvelun tai järjestelmän toimivuutta, eikä yksittäisen palvelimen tai komponentin toimivuutta.

Palvelun komponentit



Laitteet ja palvelimet

Microsoft Exchange Server 2013 on asennettu palvelimelle, jonka tarkemmat ominaisuudet on listattu alla olevissa taulukoissa.

<table>
<tr><th>Palvelin</th><th>KUSTI</th></tr>
<tr><td>Käyttöjärjestelmä</td><td>Windows Server 2012 Standard</td></tr>
<tr><td>Verkkonimi</td><td>kusti.asiakasAB.net</td></tr>
<tr><td>DNS</td><td>Sisäinen nimipalvelu:
<table>
<tr><th>Nimi</th><th>Tyyppi</th><th>Data</th></tr>
<tr><td>Kusti.asiakasAB.net</td><td>A</td><td>193.94.21.33</td></tr>
<tr><td>Kusti.asiakasAB.net</td><td>A</td><td>193.94.21.28</td></tr>
<tr><td>Autodiscover.asiakas.fi</td><td>A</td><td>193.94.21.33</td></tr>
</table>
Ulkoinen nimipalvelu:
<table>
<tr><th>Nimi</th><th>Tyyppi</th><th>Data</th></tr>
<tr><td>Mobimail.asiakas.fi</td><td>A</td><td>195.234.135.33</td></tr>
<tr><td>Autodiscover.asiakas.fi</td><td>A</td><td>195.234.135.33</td></tr>
<tr><td>Webmail.asiakas.fi</td><td>A</td><td>195.234.135.185</td></tr>
<tr><td>Mail.asiakas.fi</td><td>A</td><td>195.234.135.34</td></tr>
<tr><td>mail.asiakas.fi</td><td>A</td><td>195.234.135.35</td></tr>
<tr><td>asiakas.fi</td><td>MX</td><td>Mail.asiakas.fi</td></tr>
</table></td></tr>
<tr><td>Teho</td><td>4 vCPU, 32 GB RAM</td></tr>
<tr><td>Sisäverkon IP-osoitteet</td><td>193.94.21.28
193.94.21.33 (varattu)</td></tr>
<tr><td>Levyosiot</td><td>C 219 GB
D Data 800 GB
Mailbox database ja log levyt lueteltu alempana
X CD-ROM</td></tr>
<tr><td>Pagefile</td><td>32778Mb</td></tr>
</table>

<table>
<tr><td>Asennetut ohjelmistot</td><td colspan="5">Name: Microsoft Exchange Server
Version: 15.0.995.29</td></tr>
<tr><td>Roolit</td><td colspan="5">Exchange 2013 Mailbox, CAS, HUB</td></tr>
<tr><td>Huomautukset</td><td colspan="5">Exchange asennushakemisto:
C:\Program Files\Microsoft\Exchange Server\V15</td></tr>
<tr><td>Sertifikaatit</td><td>
<table>
<tr><th>Subject</th><th>Subject Alternative Names</th><th>Issuer</th><th>Valid to</th><th>Services</th></tr>
<tr><td>CN=
Kusti31032016</td><td>mobimail.asiakasAB.net,
kusti.asiakasAB.net,
mobimail.asiakas.fi,
AutoDiscover.asiakas.com,
AutoDiscover.asiakasAB.net,
AutoDiscover.asiakas.fi,
AutoDiscover.asiakasD.fi,
AutoDiscover.asiakasB.fi,
mail.asiakas.fi,
asiakas.com,
asiakasAB.net, asiakas.fi,
asiakasB.fi, asiakasC.fi</td><td>CN=Asiakas CA,
OU=IT,
O=Asiakas Oyj,
L=Helsinki,
S=Uusimaa,
C=FI</td><td>31.3.2018</td><td>SMTP,
IMAP,
POP,
IIS</td></tr>
<tr><td>CN=Federation</td><td>Federation</td><td>CN=Federation</td><td>26.6.2019</td><td></td></tr>
<tr><td>CN=Microsoft Exchange
Server Auth Certificate</td><td></td><td>CN=Microsoft Exchange
Server Auth Certificate</td><td>10.1.2019</td><td>SMTP</td></tr>
<tr><td>CN=kusti</td><td>kusti,
kusti.asiakasAB.net</td><td>CN=kusti</td><td>5.2.2019</td><td>SMTP</td></tr>
<tr><td>CN=WMSvc-KUSTI</td><td>WMSvc-KUSTI</td><td>CN=WMSvc-KUSTI</td><td>3.2.2024</td><td></td></tr>
</table>
</td></tr>
</table>

Sähköpostin tietokannat

Nimi	Kantasijainti	Lokisijainti
MDB10	G:\Mountpoints\MDB10\mdb10.edb	G:\Mountpoints\MDB10Logs
MDB11	G:\Mountpoints\MDB11\mdb11.edb	G:\Mountpoints\MDB11Logs
MDB12	G:\Mountpoints\MDB12\mdb12.edb	G:\Mountpoints\MDB12Logs
MDB13	G:\Mountpoints\MDB13\mdb13.edb	G:\Mountpoints\MDB13Logs
MDB14	G:\Mountpoints\MDB14\mdb14.edb	G:\Mountpoints\MDB14Logs
ADB15	G:\Mountpoints\ADB15\ADB15.edb	G:\Mountpoints\ADB15Logs
ADB16	G:\Mountpoints\ADB16\ADB16.edb	G:\Mountpoints\ADB16Logs
ADB17	G:\Mountpoints\ADB17\ADB17.edb	G:\Mountpoints\ADB17Logs
ADB18	G:\Mountpoints\ADB18\ADB18.edb	G:\Mountpoints\ADB18Logs
ADB19	G:\Mountpoints\ADB19\ADB19.edb	G:\Mountpoints\ADB19Logs

enfordb	e:\enfordb\MDB06.edb	e:\enfordb

Varmuuskopioinnit

Sähköpostijärjestelmä varmistetaan asiakkaan omaan HP Data Protector -varmistusjärjestelmään. Täysi varmistus suoritetaan päivittäin klo 15 ja kuukausittain, joka kuun 1. päivä klo 15. Erona päivittäisten ja kuukausittaisten varmistusten välillä on niiden säilytysaika.

Transport-asetukset

Globaalit asetukset

Maximum Receive size (KB)	**51200**
Maximum Send size (KB)	51200
Maximum number of recipients	5000

Hyväksytyt toimialueet

Nimi	Toimialue	Tyyppi	Oletus
asiakasAB.net	asiakasAB.net	Tärkeä	False
asiakas.fi	asiakas.fi	Tärkeä	**True**
asiakas.com	asiakas.com	Tärkeä	False
asiakasD.fi	asiakasD.fi	Tärkeä	False
asiakasC.fi	asiakasC.fi	Tärkeä	False

Sähköpostiosoitteen käytännöt

Nimi	Prio-ri-teetti	Address	Vastaanottajatyy-pit
Default Policy	Mata-lin	{X400:c=FI;a=MAILNET;p=ASIAKAS;, smtp:%rÄA%rÖO%rÅA%räa%röo%råa%g.%i.%s@asia-kas.com, SMTP:%rÄA%rÖO%rÅA%räa%röo%råa%g.%i.%s@asiakas.fi	Kaikki vastaanot-tajatyypit

Lähetysyhdistimet

Nimi	SMTP Internet	Test.local	Securemail
Lähetettävän viestin enimmäis-koko (Mt)	50	35	50
Osoitetila	SMTP:*;10	SMTP:test.local;1	SMTP:*.s;1
Lähtevän postin välittäjäpalvelin	[195.234.135.35], [195.234.135.34]	~~palikka.test.local~~	192.168.109.16

Vastaanottoyhdistimet

Nimi	Rooli	Vastaan-otetun viestin en-immäis-koko (Mt)	Mitoitus	Todenta-minen	Käytö oikeus-ryhmät
Client Frontend Kusti	Frontend-Transport	50	ALL IPV4/IPV6 PORT: 587	TLS BASIC (only after starting TLS) INTEGRATED WINDOWS	Exchange Users
Default Frontend KUSTI	Frontend-Transport	50	ALL IPV4/IPV6 PORT: 25	TLS (mutual Auth) BASIC (only after starting TLS) EXCHANGE SERVER INTEGRATED WINDOWS	Anonymous Exchange servers Legacy Exchange Servers
Outbound Proxy KUSTI	Frontend-Transport	50	ALL IPV4/IPV6 PORT: 717	TLS (mutual Auth) BASIC (only after starting TLS) EXCHANGE SERVER INTEGRATED WINDOWS	Anonymous Exchange servers
Kalevala	Frontend-Transport	50	**Use these IP addresses to re-ceive mail:** All Local IPv4 Port 25 **Receive mail from:** 77.95.150.122,193.94.21.24, 193.94.174.52, 193.94.174.200, 193.64.109.80, 192.168.76.151	TLS	

Client Proxy KUSTI	HubTransport	50	ALL IPV4/IPV6 PORT: 465	TLS BASIC (only after starting TLS) EXCHANGE SERVER INTEGRATED WINDOWS	Exchange servers Exchange users
Default KUSTI	HubTransport	50	ALL IPV4/IPV6 PORT: 2525	TLS BASIC (only after starting TLS) EXCHANGE SERVER INTEGRATED WINDOWS	Exchange servers Exchange users Legacy Exchange Servers
SMTP RELAY ALLOWED	Frontend-Transport	50	**Use these IP addresses to receive mail:** All Local IPv4 Port 25 **Receive Mail From:** 172.29.10.10, 192.168.107.91, 192.168.109.15, 192.168.109.16, 192.168.109.42, 192.168.109.45, 192.168.109.49, 192.168.110.10, 192.168.147.11, 192.168.147.24, 192.168.147.25, 192.168.198.11, 192.168.21.104, 192.168.21.105, 192.168.210.10, 192.168.31.0/24, 192.168.31.8, 192.168.32.0/24, 192.168.33.10, 192.168.33.15, 192.168.44.150, 192.168.71.0/26, 192.168.73.0/24, 192.168.74.0/24, 192.168.75.32, 192.168.76.133, 193.64.104.0/24, 193.64.105.128/26, 193.64.109.78, 193.64.109.79, 193.64.109.83, 193.64.109.85, 193.64.109.93, 193.64.109.94, 193.64.110.170, 193.64.110.171, 193.64.110.172, 193.64.110.173, 193.64.110.210, 193.64.110.70, 193.64.110.93-193.64.110.94, 193.64.110.97, 193.94.174.1-193.94.174.51,	TLS BASIC INTEGRATED	Anonymous Exchange users

			193.94.174.18, 193.94.174.193, 193.94.174.201-193.94.174.254, 193.94.174.33, 193.94.174.45, 193.94.174.46, 193.94.174.49, 193.94.174.50, 193.94.174.53-193.94.174.199, 193.94.174.57, 193.94.174.59, 193.94.174.76, 193.94.174.93, 193.94.174.97, 193.94.174.98, 193.94.21.1-193.94.21.19, 193.94.21.20, 193.94.21.21-193.94.21.23, 193.94.21.25-193.94.21.32, 193.94.21.34-193.94.21.254, 193.94.21.72, 193.94.21.78, 193.94.21.88, 253.253.253.253		

Asiakas käyttää virtualisoituja F-Secure Messaging Security Gateway -laitteita sähköpostigateway- ja roskapostinsuodatustehtävissä. Ympäristö koostuu kahdesta palvelimesta, joista toinen on konfiguraation MASTER-palvelin ja toinen palvelin on Agentti.

Palvelin	**mail1.asiakas.fi - AGENT/MAIL FILTER**	**mail2.asiakas.fi - Config MASTER**
Verkkonimi	mail1.asiakas.fi	mail2.asiakas.fi
Teho	2 CPU, 8GB RAM	2 CPU, 8GB RAM
Käyttötarkoitus	Agent, Mail Filter	Config MASTER
Käyttöjärjestelmä	Linux based OS	Linux based OS
Julkiset IP-osoitteet	195.234.135.34	195.234.135.35
Asennetut ohjelmistot	F-Secure Messaging Security Gateway 8	F-Secure Messaging Security Gateway 8

Järjestelmän toteutusdokumentaatiota ylläpidetään Elisa Appelsiinin järjestelmädokumentaatiokirjastossa apajassa, otsikolla F-secure MSG - Roskapostinsuodatus ja sähköpostigateway.

MX-tietueet

Asiakkaan käyttämät MX recordit osoittavat nimeen mail.asiakas.fi, joka on dns load balansoitu IP osoitteisiin 195.234.135.34 ja 195.234.135.35.

```
;; ANSWER SECTION:asiakas.fi.     86400  IN   MX   10 mail.asiakas.fi.;;
ADDITIONAL SECTION:mail.asiakas.fi.    86400  IN   A    195.234.135.34
mail.asiakas.fi.    86400  IN   A    195.234.135.35
```

Sertifikaatit

Status	Serial	Issued To	Issued By	Issued	Expires
Invalid, Self-signed	1277120783	mail2.asiakas.fi	mail2.asiakas.fi	2010-06-21 11:46:23 UTC+0200	2030-06-21 11:46:23 UTC+0200
Signed	0	*.asiakas.fi	DigiCert Global Root CA	2014-07-14 00:00:00 UTC+0200	2017-11-10 12:00:00 UTC+0200

SMTP-asetukset

Tekniset riippuvuudet

Sähköpostijärjestelmän riippuvuudet

VMware	Exchange asennettu virtuaalipalvelimelle Sijainti VMwaressa vcenter turbo, HKI (B-sali) / Production. Jos vmware ei toimi, palvelu ei ole saatavilla. Varmistamattomia tietoja voidaan menettää.
Active Directory	Jos AD ei toimi(domain controllereihin ei ole yhteyttä), palvelu ja hallintapalvelu eivät ole saatavilla. Active Directory sisältää tiedot kaikista ympäristön käyttäjistä,

	sekä heille määritetyistä oikeuksista ja asetuksista. Sähköpostijärjestelmä hakee tiedot suoraan AD:sta ja se ei voi toimia jos Active Directory on pois käytöstä. Samoin sähköpostipalvelimen asetukset tallennetaan Active Directoryyn. Jatkuva yhteys domain controlleriin (AsiakasAB.net) oltava.
DNS	Palvelu rajoittunut, ulkoisen nimipalvelun MX-tietue ohjaa sähköpostiliikennettä, A-tietueet yhdistää ulkoverkossa olevat asiakkaat sähköpostijärjestelmään. Sisäiset tietueet yhdistävät sisäverkon sähköposti asiakkaat järjestelmään.
Tietoliikennepalvelut	Palvelujen hyödyntämiseksi tietoliikennepalvelujen tulee olla käytettävissä. Tietoliikenneyhteyksien täytyy toimia konesalissa olevien, järjestelmään kuuluvien virtuaalipalvelinten ja loppukäyttäjien päätelaitteiden välillä. Tietoliikenneyhteyksien täytyy toimia myös ulkoverkon ja sisäverkon välillä. Aliverkot, IP-osoitteet, DHCP palvelut, kytkin, palomuuri- ja reititinkonfiguraatiot on kaikkien toimittava tai palvelut eivät ole saatavilla osittain tai kokonaan.
Levyjärjestelmät ja varmistuspalvelut	Palvelin hyödyntää vmwaressa saatavilla olevia LUNeja levyosiona ja niiden tulee olla saatavilla. Varmistuspalvelu tulee olla saatavilla. HP 3Par ja HP Dataprotector
F5	Julkaisee Exchangen sähköpostipalveluita ulkoverkon käyttäjille mobiili- ja webmail –muodossa.
F-Secure MSG	Roskapostin suodatus ja mail gateway sisään tulevan ja ulos lähtevän postin ohjaukseen.
Deltagon	Turvaposti luottamuksellisen tiedon välittämiseen

Muiden järjestelmien riippuvuudet sähköpostijärjestelmästä

Clientit	Outlook ja Outlook Web App
Lync/Skype	Kalenteritiedot
Monitoimikoneet	Skannaus sähköpostiin
Neuvotteluhuoneiden EVOKO näytöt	ews (kalenteritiedot)
Puhelinvaihteen ZyLink	ews (kalenteritiedot)

Ennakoidut vikatilanteet

Laajavaikuttaisen häiriön aikainen toiminta päätösten, organisaation ja tiedottamisen osalta tapahtuu toipumissuunnitelman päädokumentissa kuvatun prosessin mukaisesti.

Tässä kappeleessa on kuvattu käytettävissä olevat toipumismenetelmät ja seuraukset niiden käytöstä. Vikatilanteet, joihin varaudutaan sähköposti-palvelun osalta ovat:

Palvelin-ongelmat

Sähköpostikannan korruptoituminen

Sähköpostikannan tietojen korruptoituminen

Järjestelmän toipumismenetelmät vaikutuksineen on kuvattu seuraavassa kappaleessa ja käyttöohjeet kullekin menetelmälle seuraavissa kappaleissa.

Ongelmatilanne	Toipumisaikatavoite (RTO)	Toipumispistetavoite (RPO)
Exchange-palvelimen vikaantuminen	4h	24 tuntia , Viimeisin varmistus jonka perusteella palautus on tehtävissä
Järjestelmän tietokanta korruptoitunut	4h	24 tuntia, Viimeisin varmistus jonka perusteella palautus on tehtävissä
Sähköpostilaatikkoja menetetty	4h	24 tuntia, Viimeisin varmistus jonka perusteella palautus on tehtävissä

Ongelmatilanne 1, palvelin lakannut toimimasta

Jos Exchange palvelin on menetetty, ja se ei toivu esimerkiksi uudelleenkäynnistyksellä. Sähköpostipalvelut eivät ole käytettävissä, koska vikasietoisuutta ts. toista sähköpostipalvelinta ei ole.

Menetelmä 1

<https://technet.microsoft.com/en-us/library/dd876880(v=exchg.150).aspx>

6. Resetoidaan palvelimen ad-tili.
7. Asennetaan palvelimen käyttöjärjestelmä ja nimetään palvelin samalla nimellä kuin aikaisempikin Exchange palvelin oli, kts. dokumentaatio. Muulla nimellä palautus ei onnistu. Aiemmat asetukset on tallennettu Active Directoryyn alkuperäisen palvelimen nimellä. Varmista myös että palvelimeen liitetään samat IP-osoitteet kuin aiemmin. Levyt tulee osioida dokumentaation levykoot ja kirjaintunnisteet huomioiden. Alla mainittu Exchange Server recovery ei onnistu, ellei levyosiot ole samalla tavalla kuin aiemmin.
8. Liitetään palvelin toimialueelle.
9. Asennetaan tietoturvapäivitykset Wsus järjestelmän kautta.
10. Asennetaan ennalta vaaditut työkalut ja käyttöjärjestelmäkomponentit. Tarkat vaatimukset Microsoftin dokumentaatiosta Exchange 2013 system requirements and Exchange 2013 prerequisites

a) Aja seuraava komento Powershellissä

```
Install-WindowsFeature AS-HTTP-Activation, Desktop-Expe-
rience, NET-Framework-45-Features, RPC-over-HTTP-proxy,
RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-
Clustering-Mgmt, RSAT-Clustering-PowerShell, Web-Mgmt-
Console, WAS-Process-Model, Web-Asp-Net45, Web-Basic-
Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Brows-
ing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Log-
ging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-
Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-
Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-
Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Com-
pression, Web-Static-Content, Web-Windows-Auth, Web-WMI,
Windows-Identity-Foundation, RSAT-ADDS
```

c)Asenna .NET framework 4.5.2
d)Asenna Windows Management Framework 4.0
e)Asenna Microsoft Unified Communications Managed API 4.0, Core Runtime 64-bit

11. Avaa komentokehoite.
12. Navigoi Exchange 2013 asennusmedian sisältämään kansioon ja aja seuraava komento Setup /m:RecoverServer /IAcceptExchangeServerLicenseTerms
13. Asennuksen valmistuttua, mutta ennen tuotantoon asettamista, konfiguroi kaikki custom asetukset, joita aiemmalla tuotantopalvelimella oli(Kts. yo. taulukko.).
14. Uudelleenkäynnistä palvelin.
15. Palauta ja ota käyttöön tietokannat mountpointeille osion 4.2.1 mukaan.

Ongelmatilanne 2, sähköpostin tietokanta on menetetty

Exchange-sähköpostikanta korruptoitunut ja menetetty. Tällöin sähköpostipalvelut ovat joiltain käyttäjiltä kokonaan pois käytöstä, riippuen siitä onko käyttäjän postilaatikko korruptoituneessa tietokannassa vai toisaalla.

Varsinainen palautus kuvataan kohdassa 4.2.1 ja koska kyseessä on varmistuksista palautus ja se kestää yleensä useita tunteja, vaihtoehtoinen menetelmä on kuvattuna kohdassa 4.2.2. Tällä varmistetaan palvelun osittainen palauttaminen loppukäyttäjälle mahdollisimman nopeasti. Operaation jälkeen käyttäjä voi lähettää ja vastaanottaa postia, mutta ei näe vanhoja postilaatikon datoja, esimerkiksi ennen korruptiota tulleet ja lähetetyt viestit ja tallennetut kalenterimerkinnät.

Menetelmä 1, varsinainen tietokannan palautus

Ref: https://apaja.elisa.fi/display/CLIAsiakas/Palautusohjeet

1. Avaa tahma.asiakasAB.net palvelimelta "HP Data Protector Manager"
2. Valitse alasvetovalikosta "Restore", varmista että Objects –välilehti(alhaalta) on valittuna ja etsi palautettava palvelin kohdasta "Restore Objects" -> MS Exchange 2010+ Server avataan plus näppäimestä. Sen alta valitaan kusti.asiakasAB.net ja vielä MS Exchange 2010+ Server

3. Nyt oikealla puolella on Source-välilehdellä valittavan tietokannat, joista palautus halutaan suoritettavan.
4. Kun palautettava tietokanta on valittu, aukeaa Properties-ikkuna, josta valitaan esimerkiksi palautetaanko data uuteen tietokantaan vai väliaikaiseen sijaintiin. Metodeja on useita, käytämme esimerkissä ”Restore files to a temporary location”
5. Backup version kohtaan valitaan se varmistus, johon halutaan palata
6. Varmista, että Target clientissä lukee kusti.asiakasAB.net ja Restore locationiksi valitaan Kustin levy, jolla on riittävästi tilaa. Jos sellaista ei ole, lisää riittävän kokoinen levy vmwaren kapasiteetista. Jos tila on sieltäkin loppu, luo tyhjä tietokanta vanhan tilalle korruptoituneen tietokannan nimellä, https://technet.microsoft.com/en-us/library/aa997976(v=exchg.160).aspx ja valitse Data protectorin ikkunasta Restore to a new mailbox database
7. Täytä kohdat Restore into location väliaikaisella sijainnilla
8. Nimeä palautettu tietokanta tarvittaessa samannimiseksi kun se aiemmin oli
9. Kun palautus on HP Dataprotectorin mukaan valmis, aja seuraava komento konsolissa eseutil /mh <palautetun kannan nimi>.edb ja tarkista State. Jos State on Clean Shutdown, voidaan seuraava komento ohittaa
10. Jos State on Dirty Shutdown, aja eseutil /p <kannannimi>.edb ja toiminnon jälkeen varmista että State muuttui Clean Shutdowniksi
11. Jos palautus tehtiin alkuperäiseen sijaintiin, tietokannan voi kokeilla mountata, mount-database <kannan_nimi>, jos se ei onnistu
12. Jos mount ei onnistu, poistetaan korruptoituneen tietokannan kytkös Exchange management shellillä, remove-mailboxdatabase <korruptoituneen kannan nimi>
13. Lisätään varmistuksista palautettu kanta Exchange management shellillä, New-MailboxDatabase –Name <vanhan_kannan_nimi> -EdbFilePath <palautetun_kannan_polku.edb>
14. Ota tietokanta käyttöön mounttaamalla se, Mount-Database <tietokannan nimi>

Menetelmä 2, palautus mahdollisimman nopealla lähetys/vastaanotto-ominaisuuden palauttamisella

Dial-Tone Recovery

https://technet.microsoft.com/en-us/library/dd979810(v=exchg.150).aspx

1. Varmista että korruptoituneen tietokannan muut tiedostot ovat tallessa, kuten lokitiedostot jne.
2. Luo Dial-Tone tietokanta Exchange Management Shellillä, New-MailboxDatabase –Name DTDB1 –EdbFilePath G:\Dial-Tone\DTDB1.edb

3. Yhdistä korruptoitunutta tietokantaa käyttäneet postilaatikot Dial-Tone kantaan, Get-Mailbox -Database <korruptoituneen_kannan_nimi> | Set-Mailbox -Database DTDB1
4. Ota Dial Tone tietokanta käyttöön, Mount-Database –Identity DTDB1
5. Luodaan recovery tietokanta New-MailboxDatabase -Recovery -Name RDB1 -Server KUSTI -EdbFilePath " G:\Mountpoints\Recovery\RDB1\RDB1.EDB" -LogFolderPath "C:\Recovery\RDB1"
6. ja palautetaan recovery kantaan koruptoituneen kannan viimeisin toimiva versio varmistuksista käyttäen menetelmän 4.3.1 toimenpiteitä soveltuvin osin. Ennen mountia kopioi kohdan 1. lokitiedostot kohdan 5. logFolderPathiin
7. mount-database –identity rdb1 ja heti perään dismount-database –identity rdb1
8. Dismountin jälkeen kopioi rdb1 turvalliseen/varmaan paikkaan ja pidä huoli että tiedostot ovat saatavilla
9. Otetaan dial tone tietokanta pois käytöstä, Dismount-Database –Identity DTDB1
10. Siirrä dial tone tietokannan tiedostot rdb1 tietokannan kansioon
11. Siirrä RDB1 tiedostot varmasta paikasta Dial tone kannan kansioon
12. Mount-Database –Identity DTDB1
13. Mount-Database –Identity RDB1
14. Siirretään datat Revocery tietokannasta palautettuun kantaan, $mailboxes = Get-Mailbox -Database DTDB1 *ja* $mailboxes | %{ New-MailboxRestoreRequest -SourceStoreMailbox $_.ExchangeGuid -SourceDatabase RDB1 -TargetMailbox $_ }
15. Kun toiminto on valmis, voidaan RDB ottaa pois käytöstä ja poistaa se, Dismount-Database –Identity RDB1 ja Remove-MailboxDatabase –Identity RDB1

Ongelmatilanne 3, postilaatikko on menetetty

Postilaatikkoa ei millään normaalitoimenpiteellä saa käyttöön sähköposti clientissä. Ainoa vaihtoehto on palauttaa varmistuksista.

Menetelmä 1

Palautetaan varmistuksista se tietokanta, jossa postilaatikko on ja ajankohdaksi valitaan viimeisin toiminut tilanne

1. Luodaan Recovery tietokanta

```
New-MailboxDatabase-Server kusti -Name RecoveryDB -Recovery -EdbFilePath G:\Mountpoints\RecoveryDB\DB01.edb -LogFolderPath G:\Mountpoints\RecoveryDBLog
```

2. Palautetaan tietokannan tiedostot varmistuksista Recovery tietokantaan

- Luo recovery-kannalle oma mountpoint g-levylle Mountpoints kansioon. Esimerkkinä G:\Mountpoints\RecoveryDB ja G:\Mountpoints\RecoveryDBLogs ja palauta Kannan tiedosto ja lokit em. Kansioihin. Palautus tapahtuu kuten ohjeessa 4.2.1, mutta sen lisäksi palautuksen valintaikkunassa valitaan ”Restore into recovery Database”

3. Palautettu kanta Clean Shutdown tilaan: eseutil /mh <recovery-kannannimi>.edb

   - Kannan tila on Dirty Shutdown, joten ensin soft recovery: eseutil /r e01 /l G:\Mountpoints\RecoveryDBLogs /d G:\Mountpoints\RecoveryDB, jossa e01 on lokitiedostojen prefix ja edb-tiedosto on /l jälkeisessä polussa. Jos komento ei muuta tietokannan tilaa Clean Shutdown, tehdään hard recovery jossa dataa saatetaan menettää jonkin verran lokeista: eseutil /p <recoverykannannimi>.edb. Kun kanta on Clean Shutdown –tilassa, voidaan recovery kanta luoda.

4. Mountataan tietokanta

```
Mount-Database RecoveryDB
```

5. Recovery-tietokannan sisällön voi varmistaa komennolla

```
Get-MailboxStatistics -Database RecoveryDB | ft -auto
```

6. Ja yksittäisen käyttäjän postilaatikon sijainnin varmistus tietokannassa

```
Get-MailboxStatistics -Database RecoveryDB | where
displayname -eq "palautettavan postilaatikonnimi"
```

7. Koko postilaatikko palautetaan komennolla New-MailboxRestoreRequest. AllowLegacyDNMismatch on pakollinen parametri palautuksessa, jos Source ja Target postilaatikoiden nimissä eroja.

```
New-MailboxRestoreRequest -SourceDatabase RecoveryDB -
SourceStoreMailbox "palautettavan postilaatikon nimi"
-TargetMailbox korruptoituneenPostilaatikonNimi -Al-
lowLegacyDNMismatch
```

Käyttökatkon aikainen toiminta

Ongelman laajenemisen rajoittamistoimet

Tämän järjestelmän osalta ongelmien rajoittamistoimet ja niiden toteutusohjeet on kuvattu seuraavissa kappaleissa:

Ongelman rajoittamiskeino 1

Exchangen kadottaessa saapuvia posteja voidaan ulkopuolelta saapuva postiliikenne katkaista mail1.asiakas.fi ja mail2.asiakas.fi gatewaylla kunnes häiriö on korjattu. Tässä tapauksessa viestit jäävät gateway-palvelimille jonottamaan. Vaihtoehtoisesti voidaan katkaisu myös tehdä niin että mail1.asiakas.fi ja mail2.asiakas.fi ei ota postia vastaan jolloin ne jäävät jonoon lähettävän tahon postipalvelimelle.

Ongelman rajoittamiskeino 2

Palvelimen ja/tai tietokannan korruptoituminen siihen tilaan, että ne ovat palautettava edellä kuvatuissa ongelmatilanteissa, johtaa nykyisessä ympäristössä aina pitkähköön käyttökatkoon loppukäyttäjän näkökulmasta. Mahdollisesta käyttökatkotilanteesta päästään eroon kahdentamalla palvelimet/palvelut sekä muodostamalla Database Access Group -klusteri Exchange tietokannoille. Samalla riippuvuus varmistusjärjestelmästä laskee.

Tuotantokelpoisuuden testaaminen

Järjestelmän tuotantokäytön aloittaminen

Sähköpostipalvelun palautuminen normaalitilaan edellyttää teknisten riippuvuuksien toimivuutta. Virtuaalipalvelinalustan ja tietoliikenteen toiminta tulee varmistaa. Active Directory-palvelun tulee olla toimintakunnossa ja verkon nimipalvelun tulee toimia normaalisti, jotta Exchange pystyy välittämään viestejä.

Laajamittaisen ongelmatilanteen jälkeen sähköpostiliikennettä tulee testata sekä sisäverkossa, kahden tai useamman asiakkaan käyttäjän välillä. Lisäksi testataan postin kulku talon ulkopuolelle johonkin 3. osapuolen sähköposti-järjestelmään, kuten Gmailiin. Mikäli postin kulku toimii sekä ulos- että sisäänpäin, voidaan todeta että Exchange ja sähköpostin toimitukseen liittyvät vaatimukset ovat kunnossa.

Jatkotestausta voidaan suorittaa esimerkiksi tekemällä kalenterivarauksia ja -kutsuja muille asiakkaan käyttäjille. Testauksen laajuus tulee toteuttaa vallitsevan tilanteen mukaan – jos Exchange on palautettu hätätyönä katastrofin jäljiltä, on tärkeintä saada ensin sähköpostiliikenne toimimaan.